The information in this document is subject to change without notice and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. assumes no liability for damages resulting from the use of the information contained in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of that license.

Copyright © 1995-2001 by Ipswitch, Inc. All rights reserved. IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective companies.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transferred without the express prior written consent of Ipswitch, Inc.

Printing History

April 1999                      Third edition.
September 1999                  Fourth edition.
## Contents

**Preface**
- What This Package Includes
- The Ipswitch Products

**Chapter 1: Introduction**
- What is WhatsUp Gold?
- Mapping the Network
- Monitoring the Network
- Getting Information from the Network Map
- Getting Status for a Device
- Reporting
- What’s New in Version 6.0?
- System Requirements
- Upgrading
- Installation
- Trying WhatsUp Gold on Your Network
  - Creating a New Network Map
  - Adding a File Server
  - Initiating Monitoring
- Running WhatsUp Gold as an NT Service
  - Setting Up to Run as an NT Service
  - Starting and Stopping the NT Service

**Chapter 2: Creating Network Maps**
- Creating a Network Map
- Discover and Map Network Devices
- Mapping a Hierarchical Network
  - Using SmartScan
  - Results of the SmartScan
- Mapping a Flat Network
  - Results of the Scan
- Discover Devices from Network Neighborhood
- Loading a Hosts File
- Traceroute Mapping
- Manually Drawing a Map
- Reading a Network Map
  - Tips for Making a Map Easier to Read
- Device Properties
  - The Polling Method
  - Defining General Properties
  - Setting Up Monitoring
<table>
<thead>
<tr>
<th>Chapter 3: Setting Up Notifications</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining Notifications</td>
<td>56</td>
</tr>
<tr>
<td>Defining Sound Notifications</td>
<td>56</td>
</tr>
<tr>
<td>Defining WinPopup Notification</td>
<td>57</td>
</tr>
<tr>
<td>Defining Pager Notifications</td>
<td>57</td>
</tr>
<tr>
<td>Defining Beeper Notifications</td>
<td>60</td>
</tr>
<tr>
<td>Defining E-mail Notifications</td>
<td>62</td>
</tr>
<tr>
<td>Defining Group Notifications</td>
<td>64</td>
</tr>
<tr>
<td>Notification Message Variables</td>
<td>66</td>
</tr>
<tr>
<td>Testing the Notifications</td>
<td>68</td>
</tr>
<tr>
<td>Defining Program Notifications</td>
<td>68</td>
</tr>
<tr>
<td>Setting Up a Voice Modem</td>
<td>70</td>
</tr>
<tr>
<td>Defining Voice Notifications</td>
<td>71</td>
</tr>
<tr>
<td>To create a voice notification:</td>
<td>72</td>
</tr>
</tbody>
</table>

Using the Right Mouse Menu .................................................. 31
Adding a Command to the Right Mouse Menu ......................... 32
Program Variables .............................................................. 33
Custom Device Types ............................................................. 36
Creating a Custom Device Type .............................................. 36
Changing the Double-Click Action for a Custom Device .......... 39
Running a script or program for custom devices ................. 39
Using the Custom Device on a Map ....................................... 39
Scanning and Mapping a Custom Device ................................. 40
Changing the Standard Device Icons .................................... 40
Creating a Subnet ................................................................. 41
Setting Map Polling Properties ............................................. 44
Setting the Map Display ....................................................... 46
Setting Map Colors .............................................................. 47
Editing a Network Map .......................................................... 48
Getting In and Out of Edit Mode .......................................... 48
Draw Toolbar ........................................................................... 49
Keeping Tools Active ............................................................. 49
Drawing ................................................................................... 49
Attached Lines ......................................................................... 49
Creating Text Captions .......................................................... 50
Arranging the Toolbars .......................................................... 51
Saving and Naming a Network Map ......................................... 51
Saving a Context ....................................................................... 52
Assigning Notifications to Devices ................................................................. 74
Using the Alerts Icon ......................................................................................... 74
Assigning a Notification ...................................................................................... 76
Editing Notifications .......................................................................................... 78

Chapter 4: Monitoring Services ................................................................. 79
Monitoring Standard TCP/IP Services .............................................................. 81
Monitoring Custom Services .............................................................................. 83
Defining a Custom TCP/IP Service ................................................................. 83
Using Rules Expressions ................................................................................... 86
Rules Expressions Text and Quantifiers Tables .............................................. 87
Testing a Rules Expression .............................................................................. 88
Summary of Service Monitoring Requirements ............................................. 89
Custom Services API ......................................................................................... 90

Chapter 5: Working from the Console ....................................................... 91
Opening Network Maps .................................................................................... 91
Starting and Stopping Polling ........................................................................... 91
  To Initiate Automatic Polling ......................................................................... 92
  To Stop Automatic Polling ............................................................................. 92
  To Check a Device ......................................................................................... 92
Reading the Network Map ............................................................................... 93
Receiving Alarms ............................................................................................... 94
Receiving Notifications .................................................................................... 94
Acknowledging Alerts ....................................................................................... 94
Using Quick Status (Status) ............................................................................. 94
Using the Status Window ............................................................................... 96
Viewing and Changing Dependencies ............................................................ 97
  Setting “Up” and “Down” Dependencies ..................................................... 98
Viewing the Polling Statistics ....................................................................... 99
Viewing Active Notifications ...................................................................... 101
Using the Mini Status View ......................................................................... 101

Chapter 6: Logs and Reports .............................................................. 103
WhatsUp Gold Syslog ....................................................................................... 104
Logging and Reporting Events ....................................................................... 104
  Types of Events Logged ............................................................................. 104
  Changing How Events Are Logged ........................................................... 105
Viewing the Event Log .................................................................................... 107
Creating an Event Report ............................................................................... 109
Debug Log Information ................................................................................... 111
SNMP Operations ......................................................... 153
SNMP Traps ............................................................ 154
Setting Up the MIB Identifiers ..................................... 154
Viewing SNMP Objects .............................................. 156
Graphing SNMP Values ............................................. 159
Starting the SNMP Graphing Utility ............................. 160
Adding, Editing, and Deleting SNMP Objects .................. 160
Viewing Item Values .................................................. 163
Editing Item Properties .............................................. 164
Deleting Items from the Graph ................................. 165
Saving and Opening Graph Files ............................ 165
Editing Graph Properties .......................................... 166
Receiving SNMP Traps ................................................ 167
Setting Up Notifications for Traps ............................. 168
Viewing Trap Log Entries ......................................... 171
Monitoring SNMP Service ......................................... 171

Chapter 9: Using Network Tools ................................. 173
Using Format, Copy, and Print Functions ...................... 174
Printing Results .......................................................... 174
Displaying Device Information (Info Tool) ..................... 175
Checking a Web Address (HTML Tool) ......................... 176
Synchronizing Time (Time Tool) .............................. 177
Verifying Connectivity (Ping Tool) ............................ 180
Tracing a Route (TraceRoute Tool) ............................ 181
Finding Host and Name Server (Lookup Tool) ............ 184
Getting Information About Users (Finger Tool) ............ 186
Getting Owner Information (Whois Tool) .................... 187
Searching Directories (LDAP Tool) .......................... 188
Viewing Quotations (Quote Tool) .............................. 190
Scanning Your Network (Scan Tool). ......................... 191
Viewing and Graphing SNMP Values (SNMP Tool) .......... 191
Displaying Network Information (WinNet Tool) .......... 191
Testing Data Speed (Throughput Tool) ...................... 192
Viewing Local System Information ........................... 194

Index ........................................................................ 195
Preface

WhatsUp Gold is a graphical network monitoring system designed for multi-protocol networks. WhatsUp Gold monitors your critical devices and services and initiates visual and audible alarms when there’s a problem. In addition,WhatsUp Gold can notify you remotely by beeper, alphanumeric pager, e-mail, or telephone. WhatsUp Gold runs on Windows 2000, Windows NT, Windows 98, or Windows 95 on the Intel platforms.

What This Package Includes

WhatsUp Gold includes the following:

- WhatsUp Gold CD
- License agreement
- This manual, the *WhatsUp Gold User’s Guide*

The Ipswitch Products

Other Ipswitch products include:

- **WS_FTP™ Pro FTP Client**
  
  WS_FTP Pro provides two powerful Windows interfaces for connecting to remote hosts and transferring files. WS_FTP Pro includes the Find Utility, Scripting Utility, and Synchronize Utility.

- **WS_FTP Server**
  
  WS_FTP Server is a full-featured FTP server for Windows NT systems. WS_FTP Server lets you create FTP sites that make files and folders on your PC available to other users. WS_FTP Server offers many features not found in most commercial servers today, including automatic resumption of interrupted transfers.

- **IMail Server**

  IMail Server is an electronic mail server system based on Internet standards.
IMail Server provides Simple Mail Transfer Protocol (SMTP) for sending and receiving mail over the Internet or over an internal TCP/IP network. It supports any mail client that uses the Post Office Protocol, Version 3 (POP3) or Internet Message Access Protocol (IMAP4). Web Messaging lets users access their mail from any web browser; users do not need to have a mail client. IMail Server runs on Windows NT or Windows 2000 on the Intel platform.

• **WS_Ping ProPack™**

WS_Ping ProPack is the ultimate network information tool. It provides everything you need to help track down network problems and to get information about users, hosts, and networks on the Internet or on your intranet. Tools include Info, Time, HTML, Ping, Traceroute, Lookup, Finger, Whois, LDAP, Quote, Scan, SNMP, WinNet, and Throughput. WS_Ping ProPack runs on Windows NT, Windows 2000, Windows 98, or Windows 95 on the Intel platforms.
Chapter 1: Introduction

This chapter describes the basic operation of WhatsUp Gold and lists both standard and new features. In addition, you will find system requirements, upgrading and installation instructions, a quick “try it” procedure, and the procedure for running WhatsUp Gold as an NT service.

Note
For updated information since this manual was printed, see the Release Notes, WhatsUpG.txt.

What is WhatsUp Gold?

WhatsUp Gold is an easy-to-use tool for monitoring TCP/IP, NetBIOS, and IPX networks. WhatsUp Gold initiates both visible and audible alarms when monitored devices and system services go down. WhatsUp Gold can also notify you of problems by digital beeper, alphanumeric pager, sound, WinPopup, e-mail, or voice message. WhatsUp Gold provides a web interface so you can view network status from a web browser on any computer on the Internet. You can configure WhatsUp Gold and start monitoring your network without any special training.

Mapping the Network

WhatsUp Gold can map your network in several different ways, including an automatic “discover and map” capability that can scan files and the Windows network. You can also create a network map by scanning for SNMP information, scanning a range of IP addresses, loading a hosts file, scanning a network neighborhood, or drawing it.

The WhatsUp Gold scan methods:

• Poll devices on the network to which your computer is connected
• Identify any TCP/IP, NetBIOS, or IPX devices
• Create a network map with an icon for each device (workstations, servers, hosts, bridges, routers, subnets, containers, LAN boxes, hubs, printers). Each device is associated with a specific address.
Note

To scan and poll IPX devices, you must have Microsoft NWLink IPX/SPX Compatible Transport installed and running on the system on which WhatsUp Gold is installed. For more information, see “System Requirements” on page 6.

Monitoring the Network

Once you have created or loaded a network map, you can set WhatsUp Gold to continuously monitor the network, or you can initiate a single “poll” of the network. One poll of the network involves checking each monitored device in the network map. Each “check” consists of WhatsUp Gold sending a poll request to a device and tracking the response.

For each monitored device, you can choose from a set of options in the device properties to determine how the device is monitored and define what action to take if the device does not respond to a check.

On each TCP/IP device in your network map, you can determine which services are running on that device (such as HTTP, SMTP, POP3, DNS) and you can select those services you want to monitor; WhatsUp Gold monitors a service by communicating with the default port that the service runs on.
When you open the network map window, WhatsUp Gold automatically begins monitoring the network.

**Note**

Unless you have the express permission of the owners of particular devices, do not monitor host systems, workstations, or other devices that you do not control.

WhatsUp Gold is in either Monitor Mode or Edit Mode. Monitor Mode is the mode in which WhatsUp Gold polls the network. Edit Mode is the mode in which you make changes to the map; you can use Edit Mode to refine the network map, add devices, draw connecting lines, and convert icons to a different icon type. For more information, see “Manually Drawing a Map” on page 25.
Getting Information from the Network Map

In Monitor Mode, the map gives graphic indication of potential and actual problems on your network. If an event occurs such as a device going down, the name of the device becomes highlighted on the map. In addition, colors and shapes indicate the status of the various devices. By default, devices that respond to polls are displayed in green, those that have missed one poll are light green, those that have missed two polls are yellow, and those that are not accessible (or have not responded to four polls) are red. You can change the default colors and shapes. See “Setting Map Colors” on page 47.
Getting Status for a Device

In Monitor Mode, you can display up-to-the-minute status information about a device by right-clicking the device icon, then selecting **Quick Status**, and then clicking **Status**.

![Quick Status](image)

Reporting

WhatsUp Gold logs two types of data: changes in network status (called events), such as a device going down; and, polling statistics for each device.

From this logged data, WhatsUp Gold can create several reports and graphs that show the status of your network in different ways. From the **Reports** menu, you can create the following:

**Performance Graphs.** Show devices by best or worst performance based on aggregated polling statistics.

**Event Reports.** Show device up and down events, service up and down events, and WhatsUp Gold events such as map open and close.

**Statistics Reports.** Show the accumulated polling statistics by device.
What’s New in Version 6.0?

Version 6 of WhatsUp Gold offers many new capabilities:

- Web Interface now allows web security per map.
- Updated User Interface - toolbars, icons and dialogs made more user friendly and intuitive.
- Modified menu layout and context menus.
- Customizable notification plug-in system
- Map Improvements: Maps are now vector-based graphics that allow snap-to-grids, zoom in and out, and the ability to resize maps independently. Map properties now have unlimited color choices.
- Log Improvements: Improved the log file display to allow filtering, printing, saving and copying. Also improved the management of the log file size.
- Added an SNMP Viewer tool that lets you quickly view the status of interfaces on an SNMP device.
- Performance Reports now allows on-demand reporting, and the ability to generate an hourly performance report.
- Added a tool to receive Syslog messages.

System Requirements

WhatsUp Gold requires the following system resources:

- An Intel 486, or Pentium Family processor or equivalent
- Windows NT 4.0 or greater, Windows 2000, Windows 98, or Windows 95
- A TCP/IP protocol stack. Supported stacks include those from Microsoft (Windows NT, 2000, 98, 95).
- If you want to install the Performance Graphs capability, you need to first install Microsoft’s Open Database Connectivity (ODBC) interface and the ODBC text driver.

WhatsUp Gold sets up the statistics data, from which graphs are created, as an ODBC database.

ODBC is installed as part of Microsoft Office 97 or later, or you
can obtain the ODBC files from Microsoft’s web site at: www.microsoft.com/data/download_250rtm.htm.

You do not need to set up the ODBC data source. If the WhatsUp Gold installation procedure finds ODBC on your computer, it automatically sets up the data source (DSN) for Performance Graphs. The data source is wugstats.log (in the WhatsUp directory) and uses the Microsoft .txt database format.

- To scan and poll IPX devices, Microsoft’s NWLink IPX/SPX Compatible Transport must be installed and running on the system on which WhatsUp Gold is installed. You can add this transport using the Control Panel Network applet. (In the “Select Network Protocol” dialog box, select NWLink IPX/SPX-Compatible Transport and follow the online instructions.)

**Upgrading**

If you are upgrading from a previous version of WhatsUp Gold or WhatsUp, you should note the following:

- Be sure that WhatsUp Gold has completely shut down before upgrading. If you exit WhatsUp Gold during a poll, it may take up to 30 seconds for the application to be removed from memory. Until then, WhatsUp Gold appears in the Windows task list.

- Back up your network maps (.db for WhatsUp and .wup for WhatsUp Gold). When you open a WhatsUp file in WhatsUp Gold, it is automatically converted to the .wup format and saved with a .wup extension. Note that .wup maps saved in Version 6.0 cannot be used in previous versions of WhatsUp Gold.

- During installation, WhatsUp Gold will compare its own mib.txt and traps.txt files with any already present. If there is a difference, it asks if you want to overwrite your old mib.txt and traps.txt files; answer No if you have customized WhatsUp Gold to recognize vendor-provided SNMP objects.
Installation

To install or upgrade WhatsUp Gold:

1. Do one of the following:
   - If you purchased a WhatsUp Gold CD-ROM, insert the CD-ROM in a drive. If the installation program does not run automatically, then click Start, select Run, and then enter the CD path followed by AutoRun.exe. For example: 
     `d:\AutoRun.exe`
   - If you downloaded WhatsUp Gold from the Internet, run the downloaded application, `wugoldec.exe`.

2. To view a demo of WhatsUp Gold, open the map named `world.wup`.

WhatsUp Gold uses Microsoft’s Open Database Connectivity (ODBC) interface and the ODBC text driver to create performance graphs.

If the installation program finds ODBC installed on your computer, it automatically installs the Performance Graphs capability and sets up the ODBC data source to use for creating graphs.

If the installation program does not find ODBC, it asks if you want to continue the installation. If you want to use the Performance Graphs, we recommend that you:

1. Click No to cancel the installation.
2. Install ODBC (for ODBC information see “System Requirements” on page 6).
3. Restart the WhatsUp Gold installation program.

Trying WhatsUp Gold on Your Network

The following procedures let you try out WhatsUp Gold. It takes you through starting a simple network map, adding a workstation and file server, and editing the map.

Creating a New Network Map

To create a new network map:

1. From the File menu, select New Map Wizard.
2 Select **Create a blank map** and click **Finish**. 
WhatsUp Gold displays a blank map.

3 Click the **Edit Mode** button in the main toolbar, and WhatsUp Gold displays the **Edit Mode** toolbars.

4 Click the **Workstation** device in the device pool, and then drag it to the map to create an icon for the workstation.

5 Double-click the icon you just created to view device properties.

6 In the **General** dialog box, enter the information as shown. Set the **Display Name** to **ConsoleTest** or whatever name you would like for the WhatsUp Gold console (the system on which WhatsUp Gold is installed).

   The **IP Address** is **127.0.0.1**, which is the default. (This is the local “loopback” network address; it is the address you use to monitor your own system from your system.).

   **Note**
You can enter the IP Address of any device you want to monitor.

7 Click **Monitor**; make sure **Monitor This Device** is selected.

8 Click **Alerts**, select **Enable alerts**, and click **Add**. From the list box, select “Sound”, and then select “Default”. Click **OK**, and **OK** again. This sets up the default sound alert when this device goes down.
Adding a File Server

To create an icon for one of your file servers:

1. Click the **Server** device in the device pool, and then drag it to the desired location on the map to create the icon.

2. Double-click the icon you just created to view its properties.

   ![Server tool](image)

3. Click **General** and set the **Display Name** to **Server**.

4. Set the **IP Address** to the IP address, or set the **Host Name** text box to the name, of a system on your network.

   **Note**
   
   If you use a name, the network stack must be able to resolve it from a local hosts file or by looking it up on a Domain Name Server, a server that lists host names and their IP addresses. This name is looked up whenever the map is loaded.

5. Click **Monitor**; make sure **Monitor This Device** is selected.

6. Click **Alerts**, select **Enable alerts**, and click **Add**. From the list box, select “Sound”, and then select “Default”. Click **OK**, and **OK** again. This sets up the default sound alert when this device goes down.

7. Save the map from the **File** menu by selecting **Save As**. Save the map with the name of **MyTestMap.wup**.
Initiating Monitoring

You are now ready to start monitoring your little network of two items.

1. Click the **Edit Mode** button to exit Edit Mode and return to Monitor Mode.
2. Click the **Check** button to poll the network.
   
   Your screen should look something like this.

Running WhatsUp Gold as an NT Service

WhatsUp Gold can run as a system service on Windows NT 4.0 or later. When running as a service, WhatsUp Gold uses only the web interface as its user interface. To use less memory, no map windows are opened on the WhatsUp Gold NT console.

Running WhatsUp Gold as an NT service allows you to log off the NT console, thus providing an extra level of security (the service can run completely hidden.) As with any NT service, you can set WhatsUp Gold to restart whenever Windows NT is rebooted.

Setting Up to Run as an NT Service

We recommend that you create your network maps using WhatsUp Gold in normal operating mode on the Windows NT console. Once your maps are created, select any desired program options (from the **Configure** menu, select **Program Options**). These options will be in effect during operation as an NT service.
In the **Startup** dialog box, in the program options (**Configure -> Program Options -> Startup**), you can specify multiple maps to load at startup in the **Map Names** box. Make sure **Open maps on startup** is selected, and the maps listed in the **Map Names** box will load at startup. Click **Add** and select any additional maps for loading at startup. To remove any maps from loading, select the desired map(s) in the **Map Names** box and click **Delete**. Additional maps can be subsequently loaded and unloaded using the web interface, provided the maps are in the directory specified in the **Directory** box. Note that the “contexts” capability, which lets you save a particular configuration of WhatsUp Gold windows, cannot be used when operating WhatsUp Gold as an NT service.

Set any of the web server options (**Configure->Web Server->Users**). Select **Enable Web Security**. For more information about web server options, see “Chapter 7: Working from a Web Browser” on page 133.

If you set up any permissions or other web configuration parameters (set on the **General** and **Users**) while running WhatsUp Gold in normal operating mode on the NT console, you need to stop and restart the NT service mode (see section below).

On the **Users** dialog box, if you select **Automatically save user changes from web interface**, you will be able to change user options from the web interface.

**Starting and Stopping the NT Service**

Your WhatsUp Gold installation includes an executable file named `wugsvc.exe` for the purpose of installing, removing, starting, and stopping the WhatsUp Gold NT service.

To install and start WhatsUp Gold as an NT service, enter the following command at the Command Prompt:

```
wugsvc -install
```

To remove WhatsUp Gold as an NT service, enter the following command at the Command Prompt:

```
wugsvc -remove
```

Note that these two commands don’t install or remove WhatsUp Gold; they merely install and remove the NT service capability.
Chapter 2: Creating Network Maps

With WhatsUp Gold, you can use one of the automatic methods to quickly create a map of your network; then you can start monitoring your network immediately, using the default properties that WhatsUp Gold assigned to the map and the individual network devices.

However, you'll probably want to customize WhatsUp Gold so it polls your network in exactly the way that best suits your needs. This chapter describes how to do the following steps to create your map:

- Create a network map using one or more WhatsUp tools or techniques.
- View and edit the default properties for network devices (hosts, servers, etc.).
- View and edit the default map properties.
- Use Edit Mode to visually organize your network map.

Creating a Network Map

The network map is a graphical representation of the devices in a network. The following shows a typical network map.

Network devices can be workstations, hosts, servers, routers, bridges, hubs, LAN boxes, printers, subnetworks (“subnets”), containers, or custom host types.
WhatsUp Gold provides several methods and tools to create a network map and add devices to it:

- **Use Discover and Map network devices** to create a map from information on your computer or on your network. WhatsUp Gold can create a map by using a variety of information sources. A wizard steps you through the process and lets you select the "discover" method.

- **Use SmartScan** - locates devices by reading SNMP information on your network. This is the best way to discover and map a hierarchical network because it creates subnetwork maps and links them to the parent map.

- **Use Discover your network using ICMP** to automatically detect and list the devices within a specified range of IP addresses. The Scan IP can also scan each device for services (such as FTP or HTTP).

- **Use Discover devices from your 'Network Neighborhood'** to scan a Windows network (to which your computer is connected) and create a map of the devices it finds.

- **Use Import devices from a hosts file** and WhatsUp Gold creates an icon for each device found in a host file.

- **Use the Traceroute tool** to Map the route from your local system to a remote device.

- **Use File->New Map Wizard** to create a blank map, and then use Edit Mode to create devices in the map.

In all cases, after creating the map, you can organize the device icons to best represent your network by using **Edit Mode**. Edit Mode lets you draw connecting lines between device icons and add rectangles, circles, images, and text. You can use these annotation objects to group device icons and provide visual cues for identifying the different parts of your network.

You can use any combination of WhatsUp Gold methods and tools to create a network map. Each of these methods and tools is described in the following sections.
Discover and Map Network Devices

The Discover and Map capability creates a map from information on your computer — or on the network to which your computer is connected — by reading network files and identifying devices listed in the files. These files can include a hosts file, the Windows registry, and Windows network information. Discover and Map can also find devices by reading SNMP information on the network or by scanning a range of IP addresses.

To use the Discover and Map capability:

1. From the File menu, select New Map Wizard to view the following dialog box.

2. Select Discover and map network devices, and then click Next.

The Discover Devices screen appears.
Select the parameters you want to use to create the map.

**Discover your network with SNMP SmartScan.** Reads SNMP information on your default router to identify devices on your network and also identifies and maps subnets within your network. Use this option to map a hierarchical network, if your network is SNMP enabled. The Discover Devices wizard will display additional options for scanning with SNMP.

**Discover your network using ICMP.** Scans a range of IP addresses and maps the devices that respond to a message sent via the Internet Control Message Protocol (ICMP). Use this option to map a single network that does not contain subnets (all devices will be displayed on one map.) The Discover Devices wizard will display additional options for the scan.

**Discover devices from your Network Neighborhood.** If your computer is connected to a Microsoft Windows network, WhatsUp Gold scans the network and creates an icon for each device it finds. (This can take a few minutes, depending on the size of your network.)

**Import devices from your registry.** Reads the Windows registry to find devices that are referenced in the TCP/IP, Microsoft Internet Explorer, or Netscape Navigator configurations, then automatically adds the devices to the map.

**Import devices from a hosts file.** Reads the hosts file on the local system and creates an icon for each network device.

Click the **Next** button. Depending on the Discover options you selected, WhatsUp Gold does the following:

- If you selected **Discover your network with SNMP SmartScan**, it displays the “SNMP SmartScan” dialog box and asks where you want the SNMP SmartScan to start. Modify any text boxes as needed. Click **Next** to proceed. To change the default values, see “Mapping a Hierarchical Network” on page 18.
Note
To make sure you scan only those devices in your own network, you can use the Scan Depth and Limit scan to IP class of root device options. Also, the scan will stop if it comes to a network for which it does not know the SNMP Communities name.

- If you selected Discover your network using ICMP, it displays the “IP Address Scan” dialog box with default values filled in. Click Next to proceed. To change the default values; see “Mapping a Flat Network” on page 21 for more information.
- If you selected Discover devices from your Network Neighborhood, it displays the “Network Neighborhood Scan” dialog box and asks for you to pick the Domain Names you want to include in the scan. Select the desired domains and click Next to proceed.
- If you selected Import devices from a hosts file, the “Host File Import” dialog box appears and asks what host files do you want to import. Use the browse button if you want to select a different host file. Click Next to proceed.
- If you selected Import devices from your registry, the TCP/IP Service Scan” dialog box appears and asks which services do you want to scan for. Select the services for which you want to scan, and make any other changes you want. Click Next to proceed.
- Reads the network files, locates devices and displays them in the “Scan Results” dialog box. It asks which of these devices do you want to appear in the map(s). They ALL have check marks defaulted with them; only keep check marks on the devices you want to appear in the map. Click Finish and the map is created.

5 From the File menu, select Save or Save As to save the map.
**Mapping a Hierarchical Network**

If your network has a router with an SNMP agent, SmartScan is a powerful way to discover and map your network, as it can create maps and subnet maps that reflect your network’s hierarchy. SmartScan discovers and maps devices by reading SNMP data on a device (preferably a router) in your network. Based on the information it finds, SmartScan will continue to scan your network until it has mapped all devices.

To make sure you scan only those devices in your own network, you can use the **Scan Depth** and **Limit scan to IP class of root device** options. Also, the scan will stop if it comes to a network for which it does not know the **SNMP Communities** name.

**Note**

Do not scan devices on someone else’s network without their permission!

You can also enable the scan so that it discovers a custom device type and creates a custom icon for the device. For information on how to do this, see “Custom Device Types” on page 36.

A **SmartScan** can also identify network services (such as FTP, HTTP, SMTP, on each network device.

**Using SmartScan**

SmartScan maps and displays the devices according to your network’s hierarchy. If your network is divided into subnets, SmartScan creates a parent map of the top-level network and also creates a map for each subnet. The parent map will show links to its subnets, and any subnet map can have links to lower-level subnets.

To discover and map devices on your network using SmartScan:

1. If you are not already in the “SNMP SmartScan” dialog box, you can start a scan in either of the following ways:
   - To create a new map, from the **File** menu, select **New Map Wizard**. In the New Map, select the **Discover and Map Network Devices** option on the first screen and select **Discover your network with SNMP SmartScan** on the next screen.
To add devices to an existing map or a blank map, select the map, then from the Tools menu, select Discover Devices, select Discover your network with SNMP SmartScan on the next screen.

1. Edit any of the SmartScan options. Click Help for a definition of each option. Click Next to continue.

2. Select the Services you want to scan for, and click Next.

3. The scan begins and when it has completed, it provides you the opportunity to finalize which devices you want to appear on the map. Click Finish to complete the wizard.


5. From the File menu, select Save or Save As to save the map.
Note
The default settings limit the scan to your network. WhatsUp Gold provides control over these settings so that you can further limit or change the scan to reflect your unique network topology.

Note
Never try to discover and map devices on a network that is not owned by your organization!

Results of the SmartScan
SmartScan creates a map hierarchy that reflects your network and its subnets. It creates a separate map for each subnet and creates a parent map with links to the subnets.

Subnet map shows devices in the subnet’s range of IP addresses.

Parent map shows status of subnets. To open a subnet map, double-click its icon.

Note
A map created by SmartScan may show other networks connected to your network as a gray subnet icon. This means the scan was unable to map the devices in that subnet because the scan settings would not allow it.
Mapping a Flat Network

If you have one network with no subnets, or you want to create subnets manually, you can use the ICMP option.

The Scan tool automatically detects the network devices within a specified range of IP addresses and creates a single map. You specify a range of IP addresses to be scanned, and WhatsUp Gold polls each address in the range. If WhatsUp Gold finds an active network device in the range, it creates an icon for the device.

You can also enable the scan so that it discovers a custom device type and creates a custom icon for the device. For information on how to do this, see “Custom Device Types” on page 36. A scan can also identify the network services (such as FTP, HTTP, SMTP) on each network device.

To start a scan:

1. Select an existing map or create a new map window.
   - To create a new map, from the File menu, select New Map Wizard. In the New Map wizard, select the Discover and Map Network Devices option on the first screen and select Discover your network using ICMP on the next screen.
   - To add devices to an existing map, select the map, then from the Tools menu, select Discover Devices and select Discover your network using ICMP on the next screen.

2. Edit any of the IP Address Scan options. Click Help for a definition of each option. Click Next to continue.
3 Select the Services you want to scan for, and click **Next**.
4 From the **File** menu, select **Save** or **Save As** to save the map.

**Results of the Scan**

When you use the Scan tool as described above, WhatsUp Gold scans the range of IP addresses. For each active IP address it finds, it lists the address.

On the map, devices that have an SNMP service running are flagged with a triangle (monitoring SNMP) or star (is an SNMP manageable device).

Double-click the device icon and click **Services** to view Services.

(Under the right conditions, the Scan can also recognize custom device types. For more information, see “Scanning and Mapping a Custom Device” on page 40.)
Discover Devices from Network Neighborhood

The Discover devices from your Network Neighborhood option creates a map by scanning the Windows network to which your computer is connected, and finding the other devices on the network. It creates an icon for each device that it finds on the network.

To start a Network Neighborhood scan:

1. Select an existing map or create a new map window.
   - To create a new map, from the File menu, select New Map Wizard. In the New Map Wizard, select the Discover and Map Network devices option on the first screen and select Discover devices from your Network Neighborhood on the next screen.
   - To add devices on an existing map, select the map, then from the Tools menu, select Discover Devices and select Discover devices from your Network Neighborhood on the next screen.

2. Click Next to continue. WhatsUp Gold displays the possible domains for you to include in your network scan.

3. Select domains and click Next.

   WhatsUp Gold scans your Windows network and creates an icon on the map for each device that it finds. Note that this scan can take a few minutes to complete depending on the size of your network.

   **Note**
   The Scan Network Neighborhood option will also find NetWare devices.

4. From the File menu, select Save or Save As to save the map.

Loading a Hosts File

You can load a hosts file (which lists IP addresses and their associated hostnames) and WhatsUp Gold creates an icon for each device listed in the file.

1 Select an existing map or create a new map window.
   - To create a new map, from the File menu, select New Map Wizard. In the New Map Wizard, select the Discover and Map Network devices option on the first screen and select Import devices from a Hosts File on the next screen.
   - To add devices on an existing map, select the map, then from the Tools menu, select Discover Devices and select Import devices from a Hosts File on the next screen.

2 Locate the hosts file and click Next. WhatsUp Gold reads the hosts file and creates an icon for each network device it finds.

3 Select the Services you want to scan for, and click Next.

4 The scan begins and when it has completed, it provides you the opportunity to finalize which devices you want to appear on the map. Click Finish to complete the wizard.

5 From the File menu, select Save or Save As to save the map.

Creating Network Maps

The Traceroute tool lets you map the network devices (usually routers) that comprise the route of an IP packet from your local host to a remote Internet host. WhatsUp Gold displays an icon for each router and shows the connections from router to router.

For information on how to use the Traceroute tool, see “Tracing a Route (TraceRoute Tool)” on page 181.

Manually Drawing a Map

You can create network devices manually by using Edit Mode.

1 Select an existing map or create a new map window.
   To select an existing map, from the File menu, select Open and enter the map file name.
   To create a new map, from the File menu, select New Map Wizard. Select Create a blank map, and then click Finish.
2 In the main toolbar, click the Edit Mode button. The editing toolbars appear.
3 Use the drawing tools to create network devices. For more information, see “Editing a Network Map” on page 48.
4 From the File menu, select Save or Save As to save the map.
Reading a Network Map

When WhatsUp Gold is in Monitor Mode, it polls the active network maps. The icons on the map indicate the status of the various network devices. As explained in the previous chapter, when an event occurs (such as a device goes down or a trap is received) the name of the device becomes highlighted on the map. In addition, the colors and shapes of the device icons also indicate certain events as explained in “Getting Information from the Network Map” on page 4.

The indicators on the map are not the only way of getting status information about your network. The Status of a device also gives information about an individual device, and the Event Log lists all events for all open maps; both are covered in “Chapter 5: Working from the Console” on page 91.

In addition, you can get information by defining and activating notifications which are sent when particular events occur; for more information, see the following chapter.

Tips for Making a Map Easier to Read

If you have a large number of devices in your network and you used Discover and Map, Using SNMP, Using IP Addresses, or In Network Neighborhood to create a network map, the first version of the map may be a bit difficult to read. Use the tips below for making your map more readable.

- Right-click on blank space on the map and select Properties, click Display and then select Clip Names. You can also try the Wrap Names option to see if that makes the device names easier to read.
- Enter or modify the properties of the network devices. For starters, you might want to turn off monitoring for those network devices that you don’t need to monitor right away.

   To do this, double-click the device icon to view the device properties; then click Monitor and make sure Monitor This Device is cleared.
Note
To do this for a subnet icon or container icon, right-click the icon, select Properties, and click Monitor.

- Click the Edit Mode button and then drag device icons to new locations. For more information on organizing devices using shapes and lines, see “Editing a Network Map” on page 48.
- If the map contains overlapping icons, you can automatically arrange the icons on a map by clicking the Edit Mode button, and from the Arrange menu, selecting Arrange Icons. This feature arranges all icons on the current map in equally spaced rows starting in the top left corner.
- To change a device’s icon, right-click it and select Properties, click General, then select a new Type.
- You can click the Edit Mode button again to return to Monitor Mode.

Device Properties

WhatsUp Gold needs basic information about a device in order to monitor it. When you create a map using any of the “discover and map” tools, WhatsUp Gold automatically determines the device’s display name, host name, and IP address. This section describes why you might edit the default device properties that WhatsUp Gold assigns.

The Polling Method

By default, WhatsUp Gold uses the ICMP polling method for TCP/IP devices, IPX for IPX devices, and NetBIOS for NetBIOS devices. You can change the default polling method at the bottom of the General dialog box of the device properties.

- ICMP sends packets (echo requests) to a device and tracks the responses.
- TCP/IP can be used to monitor a service on a device that does not allow ICMP packets (as in the case of some firewalls). The TCP/IP setting uses either TCP or UDP to poll the service. To use this method of monitoring a device, at least one service must be monitored on that device.
• **NetBIOS** is the polling method to use for Windows networks.
• **IPX** is the polling method for Novell NetWare networks.

---

**Note**

To scan and poll IPX devices, the system on which WhatsUp Gold is installed must have Microsoft NWLink IPX/SPX Compatible Transport installed and running. For more information, see “System Requirements” on page 6.

---

If the polling method for a device is NetBIOS or IPX, you will not be able to monitor TCP/IP services on this device.

**Defining General Properties**

On the **General** dialog box, you can make any changes to general properties, change the icon type for the device, and set the method WhatsUp Gold uses to poll the device.

To view or change device properties:

1. Right-click the device and select **Properties** from the pop-up menu. Click **General**.

![General Properties Dialog Box](image)

2. In the **Display Name** text box, enter a name. This is the name displayed on the network map.

3. In the **Type** box, select the desired device type. This selection
determines which icon is displayed on the network map.

---

**Note**
The subnet icon is a special type that is used to link a subnet map to a parent map. For more information, see “Creating a Subnet” on page 41.

4 Under **Polling Method**, select the method to use for polling this device. For detailed information, see “The Polling Method” on page 27.

5 The **Poll Using** will either be **IP Address** or **Host Name**.

---

**Note**
You can toggle between **Host Name** and **IP Address**.

6 **Host Name**. If the polling method is ICMP or TCP/IP, enter either the **Host Name** here or the **IP address** in Step 5. If you enter a host name, it must be a name that can be resolved to an IP address. In other words, the host name must be in your system’s host file or in your network’s DNS server.

   If the polling method is NetBIOS or IPX, you must enter a valid NetBIOS or IPX name.

7 In the **IP Address** text box, enter a valid IP address.

   If the polling method is ICMP or TCP/IP and you entered a **Host Name** in Step 5, you can leave this blank and WhatsUp Gold will use the **Host Name** to look up the IP address.

   If the polling method is NetBIOS or IPX, leave the address blank; WhatsUp Gold displays the hardware Ethernet address of the device after it completes one poll.

8 In the **Info Line 1** and **Info Line 2** text boxes, enter any additional information about this device. This information can be included in notification messages. For example, you can enter a “point of contact” for a device or location. This information is also displayed on the Host Summary page in the web interface.

9 Click **OK** to apply the changes and exit the dialog box.
Setting Up Monitoring

You use Monitor to turn monitoring on or off for a device, to specify how often to check the device, the number of seconds to wait for a response, and any up or down dependencies.

1. In the device properties, click Monitor.

2. Make sure Monitor This Device is selected.

3. In the Poll Frequency text box, enter a value to determine how often this device should be checked. The Poll Frequency determines if this device is checked on every poll (value = 1), every second poll (value = 2), every third poll (value = 3), and so on. The default value is every poll (1), but you can use this property to poll a particular device less frequently.

4. In the Poll Timeout text box, enter the number of seconds to wait for a response from a monitored device.

   You can enter a value from 1 to 20 seconds. The default value is 5 seconds. This timeout should be set to the smallest practical value. For a local network, a timeout of 2 seconds is usually sufficient. For a long-distance (or slow-path) network, this timeout may need to be as high as 10 seconds.
5 Set the **Time Period** options to specify when you want to monitor this device. Click the *Change* button to change the default setting of 7 days a week, 24 hours a day.

Select the **Day of Week** options: *7 days a week* is the default. 
You can clear the *7 days a week* option and then select the specific days of the week that you want to monitor this device.

Select one of the three **Time of Day** options: Use *24 hours a day* to monitor all day. Use *Between* to set the start and end time for monitoring. Use *Not between* to set the hours that monitoring is turned off.

---

**Note**

When using *Between* and *Not Between*, the start time must be less than the end time. To set the period between an AM time and a PM time, you must use the 24 hour clock (0000 to 2400) or use the options together to set the hours.

Click **OK** to save your changes and exit the “Time Period” dialog box.

6 To make this device an “up dependency” for another device (meaning it gets checked only if the other device is up), select the other device from the **Check only if this device is up** list.

7 To make this device a “down dependency” for another device (meaning it gets checked only if the other device is down), select the other device from the **Check only if this device is down** list.

8 Click **OK** to apply the changes and exit the dialog box.

**Using the Right Mouse Menu**

Select a device and then click the right mouse button to display the device pop-up menu. When you’re in Edit Mode, the menu looks similar to the image to the left; in Monitor Mode, the menu has fewer commands. You can add menu commands that start applications. To do so, see “Adding a Command to the Right Mouse Menu” on
The default menu commands on the right mouse menu (in Edit Mode) are the following:

**Cut, Copy, Paste, Delete** lets you cut, copy, paste, or delete the selected device.

**New Device** lets you add devices to the map.

**Attach to** draws an attached line from the selected device to the next object you click. For information about using attached lines, see “Attached Lines” on page 49.

**Bring to Front**. If the selected item is a drawn shape, such as a rectangle or circle, this command moves it in front of all other drawn shapes.

**Send to Back**. If the selected item is a drawn shape, such as a rectangle or circle, this command moves it behind all other drawn shapes.

**Quick Status**. Takes you to the quick status dialog box where you can view the Status, History, Up-Time and Log History for this device.

**Properties** shows you the device properties.

**Adding a Command to the Right Mouse Menu**

You can add commands that start applications to the menu that appears when you right-click a device; you create these commands using **Menu** of the device properties.

To add an item to the right mouse menu:

1. Right-click a device, select **Properties** and click **Menu**.
2. Click the **Add** button and the **Edit Menu Item** dialog box appears.
3 In the **Menu Name** box, type the command as you want it to appear on the right-mouse menu.

4 In the **Command** box, enter the program name you want to start when you choose this command. You can enter the name of any executable program, or you can use one of the following values:

   - [telnet] - calls telnet.exe
   - [ping] - calls the Ping tool
   - [trace] - calls the Traceroute tool
   - [browse] – starts the default browser using the IP address as the URL

5 Following the program name, you can use arguments to pass parameters to the specified program. See the following section for a list of program variables you can use.

**Program Variables**

In WhatsUp Gold, you can call an external program:

- From the right mouse menu when you right-click a device (See “Adding a Command to the Right Mouse Menu” on page 32.)
- By double-clicking a custom device icon (See “Custom Device Types” on page 36.)
You can pass parameters to the specified program by using the variables in the following table. The specific variables you use and the order in which you use them depends on the program you are calling.

<table>
<thead>
<tr>
<th>Device Variable</th>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td>%1</td>
<td>Info Line 1 from General of device properties</td>
</tr>
<tr>
<td>%2</td>
<td>Info Line 2 from General of device properties</td>
</tr>
<tr>
<td>%a</td>
<td>IP Address from General of device properties</td>
</tr>
<tr>
<td>%c</td>
<td>Same as %T. Returns the device type. Use %T, %c was used in previous versions</td>
</tr>
<tr>
<td>%d</td>
<td>Current Date (mm/dd/yyyy)</td>
</tr>
<tr>
<td>%h</td>
<td>Display Name (from General)</td>
</tr>
<tr>
<td>%I (lower case L)</td>
<td>Display Name from General of device properties</td>
</tr>
<tr>
<td>%L</td>
<td>The Event Log file, EV-yyyy-mm-dd.tab (or %Lnn where nn=last n lines of the log file)</td>
</tr>
<tr>
<td>%Ln</td>
<td>Last n lines of the log file</td>
</tr>
<tr>
<td>%M</td>
<td>SNMP Community</td>
</tr>
<tr>
<td>%N</td>
<td>Notes and SNMP trap text. (Notes are from the device properties notes. If the event is an SNMP trap, the full SNMP trap text is appended to the notes).</td>
</tr>
<tr>
<td>%n</td>
<td>Display Name from General of device properties</td>
</tr>
<tr>
<td>%O</td>
<td>SNMP Object Identifier. Valid only for custom device types with an SNMP identifier. Returns SNMP Object identifier (from the View -&gt; Device Types dialog box) or “unknown” if SNMP Object is blank.</td>
</tr>
<tr>
<td>%p</td>
<td>Item parameter code from Add/Edit dialog box.</td>
</tr>
<tr>
<td>%R</td>
<td>SNMP Read Community from SNMP of device properties</td>
</tr>
<tr>
<td>%S</td>
<td>WhatsUp Gold status (such as “timed out” or “did not respond”)</td>
</tr>
<tr>
<td>%w</td>
<td>Winsock error code</td>
</tr>
<tr>
<td>%T</td>
<td>Device Type from General of device properties.</td>
</tr>
<tr>
<td>%t</td>
<td>Current time (hh:mm:ss)</td>
</tr>
<tr>
<td>%u</td>
<td>The word “UP” or “DOWN”</td>
</tr>
<tr>
<td>%V</td>
<td>Names of down services, followed by the word “services”.</td>
</tr>
<tr>
<td>%v</td>
<td>Names of down services</td>
</tr>
<tr>
<td>%W</td>
<td>SNMP Write Community from SNMP of device properties</td>
</tr>
<tr>
<td>System Variable</td>
<td>Returns</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>%C</td>
<td>Down Service Names</td>
</tr>
<tr>
<td>%D</td>
<td># of Down Hosts</td>
</tr>
<tr>
<td>%e</td>
<td>Down Hosts Names</td>
</tr>
<tr>
<td>%o</td>
<td># of Down Services</td>
</tr>
<tr>
<td>%P</td>
<td>Up Host Names</td>
</tr>
<tr>
<td>%U</td>
<td># of Up Hosts</td>
</tr>
</tbody>
</table>
Custom Device Types

You can create custom device types to use in a map. You can supply your own icon for these custom devices, and set them up so that they are automatically mapped when you use the SmartScan or Scan tools.

Creating a Custom Device Type

The device pool provides tools that let you add a workstation, host, server, router, bridge, hub, LAN box, container, subnet, or custom devices to your network map.

To create a custom device type:

1. If you want the SmartScan or Scan tools to use a special icon when it finds this custom device, make sure you add vendor-provided identifiers to the MIB tree, see “Setting Up the MIB Identifiers” on page 154.

2. From the Configure menu, select Custom Device Types.

![Custom Device Types dialog box](image-url)
3 Click New.

4 Enter a Template Name for the new device.

5 In the Icon Filename text box, browse to the name of an icon file that you want to use. Examples of suitable .ico and .emf files can be found in your WhatsUp Gold directory.

To edit this icon, click the Edit Device Icon button. This will open the icon in VDevice where you can edit it or just view it. See “To change one of the standard icons:” on page 41. For even more information on VDevice, see the VDevice help file.

---

**Note**

VDevice is the ONLY icon editor you can use for modifying icons.

(Optional) In the SNMP Object text box, enter an SNMP identifier (or use the browse button to find one) that corresponds to a vendor device type; this is usually found in the "private -> enterprises" section of the MIB tree, under the vendor name.

SmartScan and Scan will discover and map custom devices using the SNMP identifiers to locate the specified icons. To scan for custom devices, you must also enter the proper Community name and, if you use the Scan tool, select Identify via SNMP.

You can use multiple identifiers. For example, suppose a manufacturer named Acme makes three devices: the Acme 4500, the Acme 4501, and the Acme 4502. You could define one custom device type to represent any Acme device in the 4500 series; in the SNMP Object box, you would enter the three SNMP identifiers for the Acme 4500, 4501, and 4502.
The Scan tool will use the icon for any of the three devices. Separate multiple SNMP object identifiers by semi-colons. The last number in the identifier can be an asterisk, a range using hyphens, or contain multiples separated by commas. For example:

1.3.6.1.4.1.311.1.1.3.1.3
1.3.6.1.4.1.311.1.1.3.1.3;1.3.6.1.4.1.311.1.1.3.1.4
1.3.6.1.4.1.311.1.1.3.1.3,4
1.3.6.1.4.1.311.1.1.3.1.3-4
1.3.6.1.4.1.311.1.1.3.1.*

Note
Custom device types are stored in the hosttype.ini file. WhatsUp Gold uses the device icon for the first object identifier it finds in hosttype.ini. Thus, if a device type "Cisco 3xxx" (1.3.6.1.4.1.9.1.32-37) appears before "Cisco 3204" (1.3.6.1.4.1.9.1.37), WhatsUp Gold uses the "Cisco 3xxx" icon for the "Cisco 3204" device.

6 In the DblClk Action box, select the desired action. See “Changing the double-click action for a Custom Device” below.

7 In the AutoRun Cmd box, enter a script or program name. See “Running a script or program for custom devices” below.

8 Select the Monitoring Method (polling method) of the device. If the Monitoring Method is TCP/IP, select whatever services (you MUST select at least one) you want to monitor by default when you create a device of this type. For more information, see “The Polling Method” on page 27.

9 Services. Select the services you want this device to monitor.

10 Click OK to save the new device type.
Changing the Double-Click Action for a Custom Device

To change the action that occurs when you double-click a custom device’s icon:

- Select a preconfigured action from the list:
  - [default] - opens the device properties
  - [snmp] - starts the SNMP tool
  - [telnet] - calls telnet.exe
  - [ping] – starts the Ping tool
  - [trace] – starts the Traceroute tool
  - [browse] – starts the default browser using the IP address

- Alternatively, enter a program name in the DblClk Action text box. For example, to start WS_FTP Pro, you would enter: `ftp95pro.exe`. Enter appropriate variables to pass parameters to the specified program. See “Program Variables” on page 33.

Running a script or program for custom devices

You can set a program to run automatically whenever a scan (SmartScan or Scan) maps a custom device.

1. Enter a script or program name in the Autorun Cmd text box.
2. You can enter the same values and variables described above for “changing the double-click action.”

Using the Custom Device on a Map

To use the custom device type on a network map:

1. In the device pool, click the Custom Device Types button.
2. All custom device icons are now visible to you.
3. Click and drag the desired custom device to the map location where you want to add the custom device type.
4. After you have finished dragging the desired icons to the map, click the “Edit Mode” button to take the map back to “Monitor Mode”. Your icon(s) are now on the map.
Scanning and Mapping a Custom Device

If you want the scan (SmartScan) to identify a custom device type, such as a Cisco 4000 router, and use a custom icon for the device, you can do the following:

1 Define a custom device type. Make sure you enter the appropriate identifier in the SNMP Object text box in the “Custom Device Type Properties” dialog box.

2 If you are using Discover your network using ICMP:
   - Start a scan of the appropriate IP addresses.
   - When prompted, enter the SNMP Read Community name assigned to your network. You can enter multiple communities, separated by a comma (,). The scan checks SNMP communities in the order that they are specified.

3 If you are using Discover your network using SNMP SmartScan, enter the network’s SNMP Communities name and start the scan. You can enter multiple community names, separated by a comma (,). The scan checks SNMP communities in the order that they are specified.

If any of these conditions are not met, the scan will use one of the WhatsUp Gold standard device icons for the custom device.

Changing the Standard Device Icons

You can edit or replace the standard icons used to represent device types (workstation, host, router, etc.). If you replace a standard icon, you must use the same file name for the new file. For example, to replace the router icon, you need to call the new file “router.”

Note

We have provided you with an icon editor program. The name of this program is VDevice.exe and it is located in the program directory of WhatsUp Gold. For more information on VDevice, see the VDevice help file.

The standard icons are internal to the WhatsUp Gold program, but we have made the icon files available in the WhatsUp Gold directory. You can use these icon files as a starting point for creating your own icons.
You can use the following icon files as a starting point: bridge.emf, host.emf, subnet.emf, container.emf, hub.emf, lanbox.emf, printer.emf, router.emf, server.emf, workstn.emf

**Note**
For every .emf file in the WhatsUp Gold directory, there is also a .dse file. VDevice only edits .dse files and when saved, it will save the .dse file and also the .emf file (for WhatsUp Gold to use). DO NOT DELETE the .dse files or you will not be able to modify those icons in the future.

**To change one of the standard icons:**

1. Open one of the icon files (.dse) in VDevice.exe. You cannot use a bitmap editor.
   
   If you wanted to change the look of your printer.emf icon, you would open printer.dse.

   **Note**
   VDevice edits the .dse file and saves it and a copy of the same .emf file.

2. In VDevice, make your changes to the icon (.dse) file. Save your changes to a file with the same name as the icon you want to replace, and it will overwrite the icon file (.emf) in your WhatsUp Gold top directory.

3. VDevice replaces the internal .emf files with the edited .emf files in the WhatsUp Gold top directory.

**Creating a Subnet**

The Subnet feature of WhatsUp Gold allows you to create separate maps for different segments of your network, yet maintain a connection between the maps. If you already have a parent network map, you can create a second network map for a particular network segment and then link it to the parent map; this makes the second map a “subnet” of the parent map.
WhatsUp Gold can simultaneously monitor the parent network map and any subnet maps. When a device or service goes down in a subnet map, the subnet icon on the parent map changes color to indicate that there’s a problem in the subnet. The subnet icon in the parent network map will have the color of the highest priority alarm that occurs in the subnet map. For example, if a device in the subnet does not respond to four polls, the subnet icon is red.

To create a subnet map (assuming you already have a parent map):

1. Create a new map and add the devices for the subnet. You can use any of the methods for creating a network map described in the previous section. You can also copy and paste devices from an existing map.

2. Save the new map.

3. Open the parent map or, if it’s already open, make it active.

4. Click the **Edit Mode** button to view the editing toolbars.

5. Click the **Subnet** icon and drag it where you want to create the subnet icon.

6. Right-click the subnet icon, select **Properties**, and click **General**.

7. In the **Display Name** box, enter the file name of the subnet map, not the Map Title. This must be the name of the .wup file without the file extension. For example, if the subnet map file is named SubnetA.wup, you enter SubnetA here.

---

**Note**

Some have referred to this subnet map as the “child” map, and the map that contains the subnet icon has often been referred to as the “parent” map.

8. Click **Monitor**, make sure **Monitor This Item** is selected.

9. Click **OK**.
10 Click the **Edit Mode** button to go back to monitor mode.

When you open a network map, WhatsUp Gold can also open any associated subnet maps and start monitoring them. (From the **Configure** menu, select **Program Options->General**, and then select **Automatically load subnets when opening maps**.)

If a subnet map window is not opened, you can right-click the subnet icon and select **Load Subnet** from the menu to open it.

If a subnet map is opened but is hidden behind other windows, you can right-click the subnet icon and select **View Subnet** to bring the subnet map to the top.

**To connect a subnet map to its parent map:**

1 Right-click on a blank space on the subnet map, select **Properties**, and click **General**.

2 In the **Parent Map** list box, select the correct parent map for this subnet map (child map).

---

**Note**

If you do not tell the subnet map (child map) who the parent map is, you will not be able to go to **View**, and select **Parent Map** (it will be grayed out), nor will you see from the right-click menu on the map the choice to select **Parent Map**.
3 Click OK.
4 From within a subnet map, you can open its parent map by right-clicking and selecting View parent map, or from the View menu, by selecting Parent map.

**Setting Map Polling Properties**

You can set the polling properties for each parent network map and subnet map.

Open the map window for the network map. Right-click an empty area of the map to display the right mouse menu and then select Properties. Click General.

![Setting Map Polling Properties](image)

**Title.** This title is used to identify a network map on the Map Window and when accessed from a web browser. You should be careful about changing the Title because it is also used to report information in the Event and Statistics logs. Polling statistics are saved in the [title.wui] file. The Status, Dependencies, Statistics, and Notifications Windows display information per map and use the Title.
Poll Frequency. This is the number of seconds between the start of a poll of the map. You can enter a value in the range 10 through 3600. The status line of each Map Window displays a timer that counts down from this number to zero before starting each poll. The timer continues to count down during polls: if the previous poll is not complete when the timer reaches zero, a new poll is not started.

Default timeout. This is the number of seconds to wait for a response from a polled device. This default value is assigned to new devices when they are added to the map.

Subnet Settings. The main purpose of these settings is to set a Parent Map for the current map. If you created the map using SmartScan, then each subnet map will already have an entry for the Parent map. To change the Parent map, select any of the maps shown in the list box. This list shows all open maps.

To view a subnet’s parent map, right-click on the map, and select View parent map, or from the View menu, select Parent map.

This dialog box also shows the Network and Netmask settings for the network segment that this subnet map represents. These settings provide the default address settings for the Scan tool, if it is started when this map is active.

Network. Shows the starting IP address for this network segment.

Netmask. Shows the netmask for this network segment. The netmask defines how to read the IP address to identify subnets and devices.
Setting the Map Display

You can set the polling properties for each parent network map and subnet map.

Open the map window for the network map, right-click an empty area of the map to display the right mouse menu and then select Properties. Click Display.

Use these settings as default for new maps. If this option is selected, WhatsUp Gold applies the settings for these map properties to all new maps that you create.

Auto Resize. If this is selected, the zoom level of the map will adjust as the size of the window changes. If the window containing the map was reduced to half of the original size, the map will reduce accordingly so that you can still see the entire map. If this was not selected, as the window is reduced, the zoom level does not change and some of the map will not be visible.

Device Name. Displays the font used for the device’s display name. Click the Change Font button to open the standard Windows font selection dialog box. Select the font properties you want to use and click OK. The "Sample Label" shows the new font selection.
When Clip Names is selected, the display names for devices are terminated at the first space or period in the name, thus shortening the display name. When Wrap Names is selected, long display names are wrapped at every space or period in the name.

Setting Map Colors

To change map colors:

1. To set the default colors for each map, from the Configure menu, you select Program Options and click Map Colors.

   **Note**
   You can select custom colors for these items.

2. To change the color for an item, select the item in the Set Color For box.

3. In the Current Item Color list box, select the color that you want. The current setting for a name is displayed in the list box.

Device States

To see the default shapes and colors for devices as they miss polls, from the Configure menu, select Program Options and click Device States. If you want to change the default settings, in the Set color for column, select the device state you wish to change. After selecting it, you can change the Line Color, Fill Color, or Shape to meet your needs.

**Responding.** This is the color that indicates that a device is responding to polls. The default is solid bright green.

Note that if you change the “Responding” color, you won’t see the change until you are in Monitor Mode and WhatsUp Gold completes the next poll.

**Lost 1 pkt.** The color that indicates that a device has not responded to one poll. The default is solid light green.

**Lost 2 pkts.** The color that indicates that a device has not responded on two consecutive polls. The default is solid yellow.

**Lost 3 pkts.** The color that indicates that a device has not responded on three consecutive polls. The default is solid yellow.
Lost 4-7 pkts. The color that indicates that a device has not responded on four to seven polls. The default is solid light red.

Lost 8+ pkts. The color that indicates that a device has not responded on eight or more polls or has a network error. The default is solid dark red.

Service down. The color that indicates that a service is down on a device. The default is solid purple.

Inactive. The color that indicates a device that is not being monitored. The default is solid dark gray.

Editing a Network Map

You use Edit Mode to move device icons around in the map window. When you’re in Edit Mode, you can use tools to:

- Add and delete device icons
- Cut, copy, and paste device icons and drawn objects
- Draw, color, and size graphic shapes to visually organize network elements

Getting In and Out of Edit Mode

To access Edit Mode, make sure the map that you want to edit is active, then click the Edit Mode button in the main toolbar. The editing toolbars appear.

Note

WhatsUp Gold stops polling the network when you’re in Edit Mode.
**Draw Toolbar**

Use the Draw Toolbar to add free (unattached) lines, rectangles, filled rectangles, circles, filled circles, and text blocks to your map.

To exit Edit Mode and return to Monitor Mode, click the Edit Mode button again. The toolbars disappear.

**Keeping Tools Active**

When you're in Edit Mode, you click a tool to use it. By default, the tool stays active for one operation.

**Drawing**

To draw a shape, such as a rectangle, circle, filled rectangle, or filled circle, put the map in edit mode click the appropriate tool, and then drag on the map to create the shape. To change the default settings (line width, line color, fill color, filled, and 3D effect), right-click the shape (on the map) and select Properties.

**Attached Lines**

In addition to the freehand lines that behave like any other drawn object, you can also use attached lines.

You can attach a device to up to five other devices or drawn objects.

To attach one device to another: **Note:** You must be in edit mode.

1. Right-click the device icon you want to draw an attached line from.
2. Select Attach to. The cursor changes to a line character.
3 Click the item to which you want to attach the device.

To disconnect any attached lines that originate from the selected device:

1 Right-click the device.
2 Select Disconnect from the right mouse menu.

**Creating Text Captions**

You can use text captions to further identify a network map or segments of a map. Text is available in many fonts, sizes, text effects, and colors.

In addition, you can specify an opaque background for the text block, which is also available with a choice of colors. Text blocks can be rotated a full 360 degrees (if you select a TrueType font) to address special text labeling requirements.

To add text to the network map:

1 Click the Edit Mode button.
2 Select the Text button and click on the map where you want the text.
3 The Text Properties dialog box appears. In the Text box, replace Sample Text with the desired text.
4 Set the Text Color, Background Color, Rotation Degrees, and Font Style as appropriate.
   - **Transparent.** If this is selected, the map background color is used “behind the text”. If this is not selected, the text is set against a Background Color that you can change.
   - **Font.** Click Change Font to change the font of the text.
   - **Rotation.** Enter a number from 0 to 360 to represent the degrees to rotate the text. If you increment the numbers by clicking, you will notice the text rotating accordingly.
5 Click OK.
Arranging the Toolbars

In Edit Mode, you can arrange the WhatsUp Gold toolbars any number of ways, on or off a gray toolbar backdrop.

To make a toolbar float in its own window, drag the double gray lines at the top of the toolbar to an area off the toolbar backdrop. To move a free-floating toolbar onto the toolbar backdrop, drag its title bar to the toolbar backdrop; to use the toolbar backdrop if it’s not visible, double-click a toolbar’s title bar.

Saving and Naming a Network Map

If you save a new map from the File menu by selecting Save, the map file is saved with a default name. The first default file name assigned by WhatsUp Gold is WhatsUp.wup, and subsequent maps saved this way are named WhatsUp1.wup, WhatsUp2.wup ... WhatsUpn.wup.

To save a map with your own name, use the Save As command.
Saving a Context

You can use the Save Context function to save the window setup and locations that you have selected for monitoring a network. For example, if you regularly use a view where you have a Map Window, Tree Window, and Status Window open, you can save this view as a “context” so that you can later open the context without having to restart the Tree and Status Windows. You can use the Save Context function to save several different views of the network.

To save a context:

1. From the File menu, select Save Context. The following dialog box appears. Click New and enter a Context Name, and click OK.

2. Select one of the following start options:

   **Start as currently displayed.** When you open the context, it will be displayed as shown in the current display, with current window locations.

   **Start in Mini Status mode.** When you open the context, it will be displayed in Mini Status mode. Mini Status mode provides a simple listing of the network elements (in place of the main window) and is designed to save screen space. For more information, see “Using the Mini Status View” on page 101.

   **Start Minimized.** When you open the context, it will be displayed as an icon (minimized).

3. Optionally, select the Reload Context on Startup option if you want this context to open whenever you start WhatsUp Gold.

4. Click OK to save your changes.
To open a context:

1. From the File menu, select **Open Context**. The “Open Context” dialog box appears.
2. Select a context name.
3. Click **OK** to open the context.
Chapter 3: Setting Up Notifications

When an event occurs on your network, WhatsUp Gold performs several different actions. WhatsUp Gold:

- Records the event in the Event Log (described in “Logging and Reporting Events” on page 104).
- Updates the device properties Status and Log dialog boxes
- Changes the appearance of the device icon on a map (as described in “Reading the Network Map” on page 93).
- Optionally, sends a notification (as described in this chapter).

WhatsUp Gold can send a notification in several ways; it can:

- Sound an alarm
- Activate a beeper
- Execute a Program
- Send a message to a pager
- Send an SMTP Mail message
- Send a pre-recorded message to a telephone (only in Windows 95, 98, and only if you have a voice modem installed).
- Display a WinPopup on a Windows NT system
- Send a group of notifications that includes any of the above types

You can also set up a “recurring notification” to use a beeper, pager, or SMTP mail message to send a network status report at a specified time interval. See “Sending Recurring Notifications” on page 130.

Setting up notifications involves two steps:

1. You first need to define the notifications that you want to use, such as activating a network administrator’s beeper or sending e-mail to an individual. This section describes how to do this.

2. Then, you assign a notification to a particular device, selected devices, or all devices.

For information on assigning notifications to a device, see “Assigning a Notification” on page 76.
Defining Notifications

You define the different types of notifications using the Notifications Editor. To access the Notifications Editor:

- From the Configure menu, select Notifications Library.

Note

Any notifications you define are stored in the Notification subdirectory where WhatsUp Gold is installed.

Defining Sound Notifications

A sound notification sounds an alarm when a device or service goes down.

Note

To play the alarm sounds, you must have a sound card and speakers installed on your system. Also, do not enable sounds if you plan to run WhatsUp Gold as an NT service.

To define a sound notification:

1. From the Configure menu, select Notifications Library, and then select Sound.
2. Click Add and enter a unique Display Name for the notification.
3. In the Filename text box, Browse to the desired .wav file. There is a "Sound Recorder" button you can click to hear the sound you just selected.
4. Optionally, select the Continuous Play check box to play the sound continuously until it is manually turned off (by clicking the Quiet button on the main toolbar).
5. Click OK.
Defining WinPopup Notification

A WinPopup notification displays a message in the WinPopup window on a Windows NT system. You define one notification for each Windows NT host on which you want to display the message.

To define a WinPopup notification:
1. From the Configure menu, select Notifications Library, and then select WinPopup.
2. Click Add and enter a unique Display Name for the notification.
3. In the Destination list box, specify the Windows NT host or domain that you want to receive this notification. Note that a domain is marked with an asterisk (*).
4. In the Message text box, enter a text message plus any of the notification variables. For more information on notification variables, see “Notification Message Variables” on page 66.
5. Click OK.

Defining Pager Notifications

You can define a pager notification to send a message to a pager when a device or service goes down. WhatsUp Gold supports PageNet and other TAP (Telocator Alphanumeric Protocol) pager services, and SMS-TAP, UCP-SMS (British Telecom), and NTT pager services.

To define a pager notification action:
1. From the Configure menu, select Notifications Library, and then select the Pager.
2 Click **Add** and enter a unique **Display Name** to identify the pager notification, for example "Page Bob."

3 In the **Terminal Number** text box, enter the phone number to dial. If required, enter the pager password in the **Terminal Password** box.

4 In the **Pager ID** box, enter the pager identification number.

5 In the **Message String** text box, enter a text message plus any of the notification variables. For more information on notification variables, see “Notification Message Variables” on page 66.

6 **Protocol.** Select the type of protocol used by your pager service.

7 Click the **Port Settings** button and note the following settings:

   - **Modem Initialization String (ATEO).** The default string is ATEO. What is expected in this string are the modem commands for "Command Echo Off" (EO).
• **Baud Rate.** Select the speed (measured in bits per second) at which the serial port will communicate with the modem.

---

**Note**
Newer modems (e.g., 56K versions) may be utilized if their rate of transfer can be stepped down to a maximum of 2400 bps (TAP specification). However, some newer modems cannot be made to transfer below 9600 bps even though you may use an initialization string that specifies a lower rate of transfer.

---

• **8N1.** The TAP protocol requires the 7E1 setting for communications, but if your pager uses 8N1, you can enable this option. By default, this option is disabled.

• **Comm Port.** Select the port to which your modem is attached.

8 Click **OK** until you get back to the “Notifications Library” dialog box.

---

**Note**
Your pager should appear in the “Notifications Library” dialog box.

---

9 Click **OK** to exit this dialog box.

---

**Note**
Note: If you want to edit or delete this, select it and click on either the **Edit** or **Delete** button.
Defining Beeper Notifications

You can define beeper notifications to activate a beeper when the device does not respond to polling.

1. From the Configure menu, select Notifications Library, and then select Beeper.

2. Click Add and enter a unique Display Name to identify the beeper notification, for example, "Beep Bob."

3. In the Beeper Number box, enter the phone number to dial.

4. In the Dial String box, the default is: ATDT%s,...,%s#. WhatsUp replaces the first %s with the phone number and the second %s with the beeper code. Most modems and beepers support the use of '#' to terminate the message and '*' to print out a dash. You may find a need to increase the number of commas in the dial string if it dials the code too soon or decrease the number of commas if it waits too long.

5. In the Signal Codes section, the Up Code specifies the characters sent to the beeper to indicate that the device has come back up after being down (the default value is 0*). The Down Code specifies the code sent to indicate the device is down (the default value is 9*). The SNMP Trap Code specifies the code sent to indicate that an SNMP trap has been received for the device. (You can use the asterisk (*) character to separate codes from a
subsequent message). The **Report Message** text box is where you enter notification variables for use in recurring notifications.

When sent to the beeper, the up or down code will be followed by the Item digital code that tells you which device the notification is for. (The Item digital code is specified in the **Add/Edit Notifications** dialog box.) For more information, see “Assigning Notifications to Devices” on page 74

6 Click **Port Settings** to set the beeper communications.

   - **Dial String**. This is the default dial string used for beeper notifications.
   - **Baud Rate**. Select the speed (measured in bits per second) at which the serial port will communicate with the modem.

**Note**

Newer modems (e.g. 56K versions) may be utilized if their rate of transfer can be stepped down to a maximum of 2400 bps (TAP specification). However, some newer modems cannot be made to transfer below 9600 bps even though you may use an initialization string that specifies a lower rate of transfer.

- **COM Port**. Select the port to which your modem is attached.
- **Modem Initialization String**. The default string is ATEOQOV1X4. What is expected in this string are the modem commands for "Command Echo Off" (EO), "Result Codes On" (QO), "Verbal Results" (V1), and "Extended Status" (X4).
- **Timeout**. The timeout value determines how long the system waits after sending the last character before it hangs up the phone, if a transition is not recognized.

7 Click **OK** after you are satisfied with your Port Settings.

8 In the Beeper properties, click **OK** to save the new notification.

To test a notification, select it and click the **Test** button. WhatsUp Gold will run a test and respond with a Success or Fail message. You can view the "conversation" in the Debug log window.
Note
Since Beepers are “one way” devices (they provide no feedback to WhatsUp Gold), the Test button can return a “Success” message, even though one might not actually get the message on the beeper.

To edit a notification, select it in the list box and click Edit, and then enter your changes to the properties. Click OK to save your changes.

To delete a notification, select it in the list box and click Delete.

Defining E-mail Notifications
You can send a message to an e-mail address when a device does not respond to polling.

1. From the Configure menu, select Notifications Library, and then select SMTP Mail.

2. Click Add and enter a unique Display Name to identify the e-mail notification, for example “Mail to Netadmin.”

3. In the Mail Server box, enter the IP address of your e-mail server (SMTP mail host).
4 In the **To** box, enter one or more e-mail addresses that are accepted by the SMTP server. (This can be a simple name.) Separate each address with a comma. The addresses should not contain brackets, braces, quotes, or parentheses.

5 The **From** address defines the sender of an e-mail notification as: `<whatsup@%1>`, where `%1` is converted by WhatsUp Gold to the local hostname. If you change the default address, be sure to keep the angle brackets (`< >`) in place. Your e-mail server may require this to be a valid e-mail user.

---

**Note**

Some mail servers may fail a test message because they are looking for a "valid" e-mail address here. If this occurs, try removing the `<whatsup@%1>`, and replacing it with a "valid" e-mail address. To test this, open the Debug log (Logs->Debug Log) and watch what is transpiring between the WhatsUp Gold machine and the mail server.

6 In the **Subject** box, enter a text message or any of the notification variables.

7 In the **Message** box, enter a text message plus any of the notification variables. For more information on notification variables, see “Notification Message Variables” on page 66.

8 Click **OK** to save the new notification.

To test a notification, select it and click the **Test** button. WhatsUp Gold will run a test and respond with a Success or Fail message. You can view the "conversation" in the Debug log window.

To edit a notification, select it in the list box and click **Edit**, and then enter your changes to the properties. Click **OK** to save your changes.

To delete a notification, select it in the list box and click **Delete**.
Defining Group Notifications

A group notification includes multiple pager, beeper, group, sound, WinPopup, e-mail, or voice notifications. Each group notification can be set up to "Notify All" (send all its member notifications at once) or "Notify First" (send one member notification at a time until one is successfully sent.)

To define a group notification:

1. Select Configure -> Notifications Library and then select Group.

2. Click the Add button and enter a Group Name.

3. Add each member notification to the group by clicking the Add button to display the Add Group Member dialog box. Select from the existing notifications. Repeat until all the notification members are added.

4. (Optional) To send the member notifications one at a time until one of them is sent successfully, make sure Notify First Member is selected, and then use the Up and Down buttons to sequence the list of members.
Example A. One group notification might be named *SeriousProblem* and it might include the following four pager notifications:

- PageTodd 24 hours a day on Monday, Wednesday, or Friday
- PageElena 24 hours a day on Tuesday or Thursday
- PageKenny 24 hours a day on Saturday or Sunday
- PageManager 24 hours a day, 7 days a week

Example B. A group notification could try a series of beeper and e-mail notifications until one is successfully sent. For example, suppose you have a group notification named *Operations*; its members are:

- BeepJed
- E-mailJed
- BeepHeidi
- E-mailHeidi
- BeepFaith
- E-mailFaith

In this case, WhatsUp Gold would try to beep Jed first, but if this beeper message is *not* sent successfully, it then tries to e-mail Jed.

If the e-mail to Jed is also not successfully sent, WhatsUp Gold next tries to beep Heidi. Now, lets suppose the beeper message to Heidi *is* sent successfully; in this case, WhatsUp Gold will not attempt to send any more notifications in the *Operations* group.

5  Click **OK**.
### Notification Message Variables

In notification messages, you can use the following variables to encode information about a device.

<table>
<thead>
<tr>
<th>Device Variable</th>
<th>Returns</th>
<th>Notifications in which it is recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>%1</td>
<td>Info line 1 (from General)</td>
<td>Mail, WinPopup, Pager, Beeper</td>
</tr>
<tr>
<td>%2</td>
<td>Info line 2 (from General)</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%a</td>
<td>IP Address (from General)</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%c</td>
<td>Same as %T, returns the device type. Use %T; %c was used in previous versions.</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%h</td>
<td>Host Name (from General)</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%M</td>
<td>SNMP Community</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%n</td>
<td>Display Name (from General)</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%N</td>
<td>Notes and SNMP trap text. (Notes are from the device properties Notes. If the event is an SNMP trap, the full SNMP trap text is appended to notes.)</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%O</td>
<td>SNMP Object identifier. (Valid only for a custom device type) This is the word “unknown” if SNMP Object box is blank.</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%p</td>
<td>Item parameter code (set in the Alert setup - extra parameter for notifications)</td>
<td>✔</td>
</tr>
<tr>
<td>%R</td>
<td>SNMP Read Community (from SNMP)</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%S</td>
<td>WhatsUp Gold status (such as &quot;timed out&quot; or &quot;did not respond&quot;)</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%s</td>
<td>Winsock error code</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%T</td>
<td>Custom device Type (from General) See the Note below.</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%u</td>
<td>Can result in the word “UP”, “DOWN”, “TRAP”, “SVCUP”, or “SVCDOWN”.</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%V</td>
<td>Names of down services, followed by the word “services”</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>%v</td>
<td>Names of down services</td>
<td>✔ ✔ ✔</td>
</tr>
<tr>
<td>%W</td>
<td>SNMP Write Community (from SNMP)</td>
<td>✔ ✔</td>
</tr>
</tbody>
</table>
### Setting Up Notifications

**Note**

The System Variable related fields are used by any notification at any time. They are particularly useful for recurring notifications. The Device Variable related fields will be filled with valuable data only if the notification was triggered by an alert. They will not be resolved if used in recurring notifications.

<table>
<thead>
<tr>
<th>System Variable case sensitive</th>
<th>Returns</th>
<th>Notifications in which it is recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>%C</td>
<td>Down Service Names</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%d</td>
<td>Date format is (mm/dd/yyyy)</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%D</td>
<td># of Down Hosts</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%e</td>
<td>Down Host Names</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%L</td>
<td>The Event Log file, EV-yyyy-mm-dd.tab (or %Lnn where nn = last nn lines of the log file)</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%Ln</td>
<td>Last n lines of the log file (n can go up to 99)</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%l</td>
<td>Local Host Name</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%o</td>
<td># of Down Services</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%P</td>
<td>Up Host Names</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%t</td>
<td>Current time (hh:mm:ss)</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
<tr>
<td>%U</td>
<td># of Up Hosts</td>
<td>Mail WinPopup Pager Beeper</td>
</tr>
</tbody>
</table>
Testing the Notifications

To test a notification, select it in the Notification Editor and click the Test button. WhatsUp Gold runs a test and responds with a Succeeded or Failed message.

You can open the Debug Log (Logs->Debug Log) to see the conversation.

Defining Program Notifications

You can define Program notifications to launch an application when a device goes down or comes back up.

1. From the Configure menu, select Notifications Library, and then select Program.

2. Click Add and enter a unique Display Name to identify the program notification.
3 In the **Program Filename** box, enter the executable name of the application you want to launch. Use the browse button to help you do this.

4 In the **Working Path**, specify a directory where the working files for the application are stored. Use the browse button to help you do this.

5 In the **Program Arguments** box, enter any program variables you want to pass to the specified program. For more information on notification variables, see “Notification Message Variables” on page 66.

6 Click **OK** to save the new notification.

To edit a notification, select it in the list box and click **Edit**, then enter your changes to the properties. Click **OK** to save your changes.

To delete a notification, select it in the list box and click **Delete**.
Setting Up a Voice Modem

To use voice notifications, you must install a supported voice modem and the Unimodem/V drivers on the system on which WhatsUp Gold is installed. WhatsUp Gold has been tested with the 3COM/US Robotics Sportster Voice56K Faxmodem with Personal Voice Mail, and the older 33.6K modem.

Note
At the time this manual was published, the Unimodem/V drivers were supported on Windows 95 and 98 only. Therefore, you cannot use voice notifications on Windows NT, or Windows 2000.

To install the driver and voice modem:

1. Download the Unimodem/V driver, unimdv.exe, from Microsoft. Copy it to an empty directory and run it to extract several files. See the readme.txt for installation instructions.

2. If your voice modem is not directly supported by Unimodem/V, go to your modem manufacturer’s web site and locate the Unimodem/V support files and .wav driver. Copy the proper .inf files into your windows\inf directory, open the Windows Explorer to the directory, select the files, and select Install from the right mouse menu (or read the vendor’s instructions).

Note
Newer modems (56K) will probably already have this driver.

3. If the WhatsUp Gold .wav files are compatible with your modem, you can use them. If they’re not compatible, or you want to change the message, you can record new files. The suggested default setting for recording is: PCM 8,000 Hz, 16 bit, Mono.
Wave files needed for voice notifications are:

<table>
<thead>
<tr>
<th>Default .wav file</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>isdown.wav</td>
<td>&quot;... is down.&quot;</td>
</tr>
<tr>
<td>isup.wav</td>
<td>&quot;... is now reachable.&quot;</td>
</tr>
<tr>
<td>svcdown.wav</td>
<td>&quot;a service is down on ...&quot;</td>
</tr>
<tr>
<td>svcup.wav</td>
<td>&quot;the service is now up on ...&quot;</td>
</tr>
<tr>
<td>ahost.wav</td>
<td>&quot;a host ...&quot;</td>
</tr>
<tr>
<td>pressone.wav</td>
<td>&quot;WhatsUp has a message for you. Press 1 for the message.&quot;</td>
</tr>
</tbody>
</table>

4 Set the .wav files on the **Voice** dialog box to point to the .wav files that you create.

For more information, see the following section, “Defining Voice Notifications.”

5 Make sure your serial port has a COM driver.

You can check this in the Control Panel by selecting **System -> Device Manager -> Ports ->** (modem’s COM port).

**Note**

If you do not have all of the above installed (voice modem, Unimodem/V drivers, and a COM driver), you will not see the **Voice** icon in the “Notifications Library” dialog box.

**Defining Voice Notifications**

After setting up the voice modem (see previous section), you can define voice notifications to send a voice message to a telephone or answering machine when a device goes down or comes back up.

You can use the default .wav files included with WhatsUp Gold to send a message, or you can record your own .wav files.

When a voice notification is triggered, WhatsUp calls the specified telephone number and plays the initial message.

The default initial message (pressone.wav) is “WhatsUp has a message for you. Press one for the message.” When you press 1 on the phone, one of the up or down messages will play, such as “A host is down.”
If you want to include the device name in the message (for example, “Gyro is down”), you can record a .wav file of a particular device name and enter the .wav file name in the “Add Notifications” dialog box when you add the voice notification to that device.

For more information, see “Assigning Notifications to Devices” on page 74.

**To create a voice notification:**

Note
The Voice dialog box is displayed only if the system has a voice modem and the Unimodem/V driver installed.

1. From the **Configure** menu, select **Notifications Library**, and then select **Voice**.
2. Click **Add** and enter a unique **Display Name** to identify the voice notification.
3. In the **Phone number** box, enter the phone number to dial.
4. In the **Repeat Msg** box, enter or select the sound (.wav) file that will be played as the initial voice message to tell the recipient that they have received a message from WhatsUp Gold. Click the **Invoke Sound Recorder** button to open the .wav file in the Sound Recorder. You can play the sound file or edit it to create a different sound.
5. In the **Count** box, enter the number of times to play the initial message (if the message is not acknowledged).
6. In the **Button** box, enter the number on the telephone that the recipient presses to get the status message.

The default message tells the recipient to press 1 to receive the status message. You can set this number to 99 to make it accept any number pressed on the telephone.
Setting Up Notifications

WhatsUp Gold

Note
If a voice mail or an answering machine answers the phone, the voice notification will not get beyond the initial .wav file (specified in the Repeat Msg box).

Optionally, enter the sound (.wav) file that will be played for any of the status messages or WhatsUp Gold will use the default status messages

Note
Click the Invoke Sound Recorder button to open the .wav file in the Sound Recorder. You can play the sound file or edit it to create a different sound.

- **Item Down.** Browse to the desired .wav file you want to play when the device on the map goes down.
- **Item Up.** Browse to the desired .wav file you want to play when the device on the map comes back up.
- **Service Down.** Browse to the desired .wav file you want to play when a service being monitored by a device goes down.
- **Service Up.** Browse to the desired .wav file you want to play when a service being monitored by a device comes back up.

The default status messages are:

<table>
<thead>
<tr>
<th>Property</th>
<th>Default .wav file</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Down</td>
<td>isdown.wav</td>
<td>&quot;... is down.&quot;</td>
</tr>
<tr>
<td>Item Up</td>
<td>isup.wav</td>
<td>&quot;... is now reachable.&quot;</td>
</tr>
<tr>
<td>Svc Down</td>
<td>svcdown.wav</td>
<td>&quot;a service is down on ...&quot;</td>
</tr>
<tr>
<td>Svc Up</td>
<td>svcup.wav</td>
<td>&quot;the service is now up on ...&quot;</td>
</tr>
<tr>
<td>Wave file (in Alerts)</td>
<td>ahost.wav</td>
<td>&quot;a host ...&quot;</td>
</tr>
</tbody>
</table>

7 Click OK.
Assigning Notifications to Devices

**Note**
Before you can assign a notification to a device, you must define the notification. For more information, see “Defining Notifications” on page 56.

WhatsUp can notify you when:

- A device is down
- A service on a device is down
- An SNMP trap has been received for a device

In order to receive a notification for one of these events, you need to *define* the notifications you want to use. Then, once you have defined the notifications, you *assign* them to the appropriate device(s). These can be individual devices, selected devices, or all devices in a particular network map.

**Note**
Assigning notifications to a group of devices overrides notifications assigned to individual devices. Therefore, assign notifications to the group *before* you assign them to individual devices.

**Using the Alerts Icon**
You use the **Alerts** dialog box to:

- Enable logging
- Enable an alarm sound
- Assign notifications and/or enable notifications

To use **Alerts**:

1. Double-click the device to view the device properties, and then click **Alerts**.

**Note**
**NOTE:** To do this for a subnet icon or container icon, right-click the icon, select **Properties**, then click **Alerts**.
2 If alerts are not enabled and no notifications are assigned, the Alerts dialog box is similar to the following:

![Alerts dialog box]

If notifications have been assigned to the device, they appear in the list box. If the notifications are enabled, they appear in a black font, but if they were assigned and subsequently disabled, they appear in gray. Each device can have up to 10 notifications.

3 Make sure Enable Alerts is selected.
4 If you want to log “UP” and “DOWN” events for this device, make sure Enable Logging is selected. These entries can be viewed on the Log dialog box of a device. (Right-click the device, select Quick Status and then select Log.)

Assigning a Notification

**Note**
Before you can assign a notification to a device, you must define the notification. For more information, see “Defining Notifications” on page 56.

To assign a notification, you add it to the list box on the Alerts dialog box (if Enable alerts and Enable Notifications are selected):

1 On the Alerts dialog box (right-click a device, select Properties, and then click Alerts), click the Add button to view the “Add Notifications” dialog box. The appearance of this dialog box varies slightly depending on the notification that is selected in the list box at the top of the dialog box.

![Add Notification Dialog Box](image)

2 Select a defined notification, from the list box. All your defined notifications are available from this list.

**Note**
To play the alarm sounds, you must have a sound card and speakers installed on your system. Also, do not enable sounds if you plan to run WhatsUp Gold as an NT service.
3 Enter a **Trigger**. WhatsUp Gold sends the selected notification after this number of failed checks. We recommend that this number be at least 4.

4 (Optional) **Auto send UP alert after sending DOWN alert.**
   When selected, the notification is sent when the device or service comes back up after a down notification. (Valid for all notifications except sound notifications).

5 **Send alert even if console response.** When checked, any active notifications for the device will be sent even if the alarm has been turned off on the WhatsUp Gold console (by clicking the **Quiet** button in the main toolbar).

   **On SNMP Trap.** When this option is enabled, and the edit box to the right of it is empty, the specified notification will be sent when any SNMP trap is received for the device. If the edit box contains a trap number or numbers, notification is sent only if a trap with the specified number is received. Separate multiple entries in the text box with a comma. For more information on SNMP traps, see “Monitoring SNMP Service” on page 171.

   You can enter a number for one of the six standard traps. If you are unsure of a trap number, you can view the Events Log (after enabling traps) to see what number is associated with a particular trap.

6 **Time Period.** Specify when you want to receive notifications from this device. Click **Change** to change the default setting of 7 days a week, 24 hours a day.
Device Identifier: Enter any information you want to associate with this specific notification type. For example, you would enter an Item digital code for a beeper. For a voice notification you would enter a wave file. Other specific notifications may use this identifier in different ways.

- For a beeper, this is a unique numeric code that identifies the device (for example, the IP address). This code is sent to the beeper following an "Up" or "Down" code. It is only valid for beeper notifications. Note: You can use the asterisk (*) character to separate numbers in an IP address.

- For a voice notification, this is a wave file that identifies the device (for example, your recorded voice). To do this, record a .wav file for the device; for example, the recording could say "Server one." When the device goes down, the voice message will be "Server one is down." The default method ([auto]) is to look for the file display_name.wav (for example, server1.wav). If the file is not found, it plays the file ahost.wav, which says "a host," as in "A host is down."

### Editing Notifications

You can edit:

- The way a notification works with a particular device
- The basic definition of a notification

To edit the way the notification works with this device, select the notification on the device properties Alerts dialog box and click the Edit button to see the “Edit Notification” dialog box. (This is essentially the same dialog box used in adding a notification.)

**Note**

Follow the instructions as specified in “Assigning a Notification” on page 76.
Chapter 4: Monitoring Services

When WhatsUp Gold checks a device, it also checks each service you have selected to monitor on the Service dialog box of the device properties. WhatsUp Gold can monitor:

- Standard TCP/IP services
- Nonstandard TCP/IP services such as those that use nonstandard port numbers (for example: Radius or IRC)
- Any other services (such as NT system services) that can be checked by a custom, user-defined module using Microsoft’s Component Object Model interface. See “Custom Services API” on page 90.

When a monitored service misses a poll, you have several ways of knowing about it:

- An event is automatically recorded in the Event Log and on the Log dialog box of the device properties. This Log dialog box is found by right-clicking on a device, selecting Quick Status, and then clicking Log.
- The Status dialog box of device properties is automatically updated. This Status dialog box is found by right-clicking on a device, selecting Quick Status, and then clicking Status.
- The device icon on the network map automatically changes color to purple (provided you are using the default colors).
- (Optional) A notification is sent. (This happens if a notification is assigned to the device on which the service is running.)

Note
Using WhatsUp Gold to monitor a service that is logged by another application may increase the size of that application’s log files by generating entries to those files. Also, the other application may view the WhatsUp Gold checks as failed connections; this could negatively impact statistics generated from the other application’s log files.
To reduce the load on your network, we recommend you monitor only the most critical services, and not every service on a device.
Monitoring Standard TCP/IP Services

Standard TCP/IP services include DNS, FTP, POP3, SMTP, HTTP, IMAP4, NNTP, SNMP, Echo, Gopher, Telnet, and Time. You can scan a device to see which of these standard services are running on it.

To scan a device to see what services are running:

1. Double-click the device to view its properties.

   **Note**
   
   To do this for a subnet icon or container icon, right-click the icon, select **Properties**, and click **Services**.

2. Click **Services**.

3. Click the **Auto Discover** button.

   Any services found are selected (check mark is displayed) for monitoring.

The Services dialog box before clicking the Scan button shows two services being monitored.

After clicking the Scan button, the dialog box shows three additional services running on the device.

By default, WhatsUp Gold monitors services using ICMP packets, but if you want to monitor a service on a device that does not allow ICMP packets, you need to change the **Polling Method** from **ICMP** to **TCP** on the **General** dialog box of the device properties.
The TCP setting uses either TCP or UDP to poll the service. To use this method of monitoring a device, at least one service must be monitored on that device.

Services can be monitored only on a device that has ICMP or TCP selected as the Polling Method (on the General dialog box of the device properties). In other words, if you have selected IPX or NetBIOS as the polling method for the device, you cannot monitor the TCP/IP services on that device.

You indicate what TCP/IP services you want to monitor on the Services dialog box of the device properties.

1 Double click a device to view its properties. Click Monitor and select Monitor This Device.

2 Click Services.

Note
To do this for a subnet icon or container icon, right-click the icon, select Properties, and click Monitor and select Monitor This Device.
3  Select the services you want to monitor.

On the Services dialog box, you can click the Auto Discover button to scan the device and see which of the standard services are running on it: WhatsUp Gold selects all active services it finds.

4  Click OK to save changes.

**Monitoring Custom Services**

You can also monitor “custom” services. Custom services include:

- TCP/IP services that are not listed on the Services dialog box (such as Radius or IRC)
- TCP/IP services that use a nonstandard port number

You can define an unlimited number of TCP/IP custom services; these become dynamic, sharable objects that can be monitored on any device on any network map.

WhatsUp Gold is shipped with custom services already defined for you:

- HTTP Content Scan
- Radius Server (Remote Authentication and Dial-In User Service)

You can define additional TCP services. For example, you may want to monitor an IRC (Internet Relay Chat) service, a Lotus Notes server, a Microsoft SQL server, or a Microsoft Exchange service.

**Defining a Custom TCP/IP Service**

The monitoring of a service always involves a protocol handshake and can also include some additional information exchange between WhatsUp Gold and the service. You can search the response from the service for an exact match of a particular text string, or you can use rules expressions to analyze the response for a more generic text pattern.

For example, if you are looking for any error message, and you know that all possible error messages have the word “fail” in common, you can use a rule expression to look for just the word “fail.” Or, you can create a rule expression that looks for any number of possible error messages. (You can search for “this,” “that,” or “the other.”).
To define a custom TCP/IP service:

1. From the **Configure** menu, Select **Custom Services**. You see the following dialog box.

   ![Custom Monitoring Services dialog box](image)

   The list box shows the custom services that are already defined.

2. Click the **New** button.

   ![New Service dialog box](image)

3. From the **Service Type** list box, select **TCP/IP Service**.

4. In the **Service Name** text box, enter a unique name for the service. This name will be displayed as a selectable option on the **Services** dialog box of the device properties. Click **OK** to return to the “Custom Services” dialog box shown above. The name you entered for the new service now appears in the **Name** list.

5. In the **Name** list, select the name you just entered.

6. The **Network Type** is **TCP** (as you established in step #3).

7. In the **Port Number** text box, enter the TCP or UDP port that you wish to monitor. For example, 6667 is the standard port for IRC.

8. In the **Timeout Seconds** text box, set the timeout for the service status, in seconds. Note that this is different than the timeout used for polling a device.
9 In the **Expect on connect** text box, enter a text string or a rule expression that you expect the remote service to send back to you on connect. For information on composing a rule expression, see “Using Rules Expressions” on page 86.

10 In the **Send command on connect** text box, enter the command to send to the service’s port.

**Examples:**

For IRC, the command is

```
Version\r\n```

For HTTP, the command is:

```plaintext
GET /Access/myprogs/dbstat.qry HTTP/1.0\r\nAccept:*/*\r\nUser-Agent: Ipswitch Whatsup/6.0\r\n```

(This is for a cgi program named `dbstat.qry` located in `/Access/myprogs/`; this program performs a status check of a database.)

11 In the **Expected command response** text box, enter text or a rule expression that represents the expected response to the send command. For example, for IRC, this is

```
:irc
```

For the HTTP example above, you might scan for an approximate match by using:

```
.*(successful|success|ok)
```

You can enter a customized string that you have set up on the service to tell you that everything is OK. For more information, “Using Rules Expressions” below.

12 In the **Send to disconnect** text box, enter a command string to disconnect from the service properly. For most TCP/IP servers, the string `QUIT\r\n` is proper. If a command string is not specified, the connection is closed by sending a FIN packet and then an RST packet.

13 Click **OK**.

---

**Note**

You **must** click the **OK** button to save the custom service.
Using Rules Expressions

The rule expression syntax is:

\[ \text{search_text} \quad \text{quantifier} \]

Note that \text{search_text} can be any combination of literal text and the text patterns shown below.

To create a rule expression:

1. In the “Custom Services” dialog box shown on page 84, click the Browse button next to Expect on connect or Expected command response to view the Rules Expression Editor.

2. Select the contains option to look for messages that contain the search string; select Doesn’t contain to look for messages that do not contain the search string.

3. Select Match Case to search for text that matches the case of the search string; to ignore case, make sure Match Case is cleared.

4. Enter the expected text by doing one or more of the following:
   - Type the literal text that you want to search for. For example, if you want to find the word fail, type fail.
   - Type the text and quantifiers you want to search for; See “Rules Expressions Text and Quantifiers Tables” on page 87.
   - Click Insert Expression or Insert Quantifier to insert a generic form of a text pattern or a quantifier. Then edit the inserted expression. See “Rules Expressions Text and Quantifiers Tables” below.

5. Click OK to save the rule.
## Rules Expressions Text and Quantifiers Tables

<table>
<thead>
<tr>
<th>Text Pattern</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match any character</td>
<td>.</td>
</tr>
<tr>
<td>Match X or Y</td>
<td>(x/y)</td>
</tr>
<tr>
<td>Match any word character (a-z, A-Z, 0-9)</td>
<td>w</td>
</tr>
<tr>
<td>Match any non-word character</td>
<td>W</td>
</tr>
<tr>
<td>Match any digit (0-9)</td>
<td>$d</td>
</tr>
<tr>
<td>Match any non-digit</td>
<td>$D</td>
</tr>
<tr>
<td>Match any white space (spaces and/or tabs and/or carriage returns)</td>
<td>$s</td>
</tr>
<tr>
<td>Match any non-white space</td>
<td>$S</td>
</tr>
<tr>
<td>Match any punctuation character (any character other than \w or \s)</td>
<td>$p</td>
</tr>
<tr>
<td>Match any non-punctuation character</td>
<td>$P</td>
</tr>
<tr>
<td>Match '.'</td>
<td>.</td>
</tr>
<tr>
<td>Match Binary value</td>
<td>%nnn where nnn is a number between 0 and 255</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quantifier</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Zero or more</td>
<td>*</td>
</tr>
<tr>
<td>Match One or more</td>
<td>+</td>
</tr>
<tr>
<td>Match n times</td>
<td>{n}</td>
</tr>
<tr>
<td>At least n, but not more than m (where n and m are numbers)</td>
<td>{n,m}</td>
</tr>
</tbody>
</table>

Note: As shown above, the following characters have special meaning in a rule:

```
( ) | * + . : %
```

If you want to use one of these characters in a search string, precede it with a backslash. For example, to search for a plus sign, enter \+ in the search string.
Testing a Rules Expression

To test a rule expression, you use the Rules Expression Editor.

1. If the Rules Expression Editor is not visible, from the Configure menu, select Custom Services. Then, select the rule you want to test. Click the Browse button next to the rule to view the Rules Expression Editor.

2. In the lower text box of the Rules Expression Editor, copy a message that meets your intended search criteria, select Contains, and click Test Expression.

If the rule expression does what you intended it to, The Comparison Text MATCHED the Pattern Specified is displayed.
If the rule expression *doesn't* test true, **The Comparison text DID NOT MATCH the pattern specified** is displayed. Edit the rule expression and test again. For a long or complex rule expression, we recommend you test one part of it at a time.

**Summary of Service Monitoring Requirements**

When you want to monitor services (either standard or custom), you need to make the following changes to the device properties:

- On the Monitor dialog box of the device properties, select **Monitor This Device**
- Use the Service dialog box of the device properties to select the **Services to Monitor** on the device.
Custom Services API

WhatsUp Gold provides a COM interface to allow experienced COM program developers to create customized service checks that “plug in” to WhatsUp Gold. In fact, the TCP/IP Service monitoring capability of WhatsUp Gold is implemented as a plug-in module that uses WhatsUp Gold’s COM interface.

You can also visit our web site and download other plug-ins such as an NT Service Monitor Plug-In and an SNMP Threshold Plug-In. Any other plug-in modules we make available in the future will also be listed on our web site.

To write your own plug-in modules, see the wugapi.h file that was installed with WhatsUp Gold.

Note

All pertinent information regarding the implementation of the COM interface is provided in the wugapi.h file that is automatically installed in the WUG program directory. The information in this file is for experienced COM program developers to use to extend the monitoring capabilities of WhatsUp Gold. It is beyond the scope of this document to provide any guidance on writing COM applications.
Chapter 5: Working from the Console

WhatsUp Gold device pool has two interfaces: the console and the web interface. The WhatsUp Gold console is the system on which WhatsUp Gold is installed.

This chapter describes how to use the console to start and stop polling of the devices in your network map and how to display network status. “Chapter 7: Working from a Web Browser” tells you how to use WhatsUp Gold from the web interface.

Opening Network Maps

In order for WhatsUp Gold to monitor a network, you need to have the network map open. You can open previously-defined maps [File- >Open] or create a new network map [File->New Map Wizard]. For detailed information on creating a network map, see “Chapter 2: Creating Network Maps” on page 13.

You can open multiple map windows and WhatsUp Gold can monitor the network maps simultaneously. If you open a map that contains subnets, the subnet maps will also open.

For any device that you do not want to poll, you can clear Monitor This Device on the Monitor dialog box of the device properties. (The icon for any device that is not being actively monitored is displayed in dark gray by default.)

Starting and Stopping Polling

When you open a network map, Whatsup Gold immediately starts automatic polling — it polls the devices continuously, starting each new pass after a specified time interval. If a map contains subnet maps, WhatsUp Gold also opens the subnet maps and starts polling. You can stop and start automatic polling at any time.

You can also start a single check of the network, in which case WhatsUp Gold makes a single pass through the devices in the active network map, polling each device.
To Initiate Automatic Polling

When you open a network map, Whatsup Gold immediately starts automatic polling on the map and any associated subnet maps.

To change the default settings for automatic polling, right-click a blank space on the map and select Properties. The map properties appear. Click General and set the number of seconds you want between checks (Poll Frequency), the number of seconds to wait before timeout (Default Timeout), and any other options you may want to change.

If polling is stopped, you can restart automatic polling of currently active devices by clicking the Stopwatch button in the main toolbar. WhatsUp Gold checks each device and tracks the responses. After waiting the time set in the Poll Frequency, it makes a second polling pass through the devices and continues polling until you stop polling by clicking on the Stopwatch button again or by closing the map window.

WhatsUp Gold polls the devices in the order in which they were created in the network map. To view or change the polling sequence, from the View menu, select Dependencies. For more information, see “Viewing and Changing Dependencies” on page 97.

To Stop Automatic Polling

To temporarily stop automatic polling, click the Stopwatch button in the main toolbar. To resume polling, click Stopwatch again.

Note

If you exit WhatsUp Gold during a poll, it may take up to 30 seconds for WhatsUp Gold to remove itself from memory. Until it is removed from memory, WhatsUp Gold appears in the Windows task list (when you press Ctrl+Alt+Del).

To Check a Device

To do an immediate poll of a device, right-click a device and select Check now from the pop-up menu.
Reading the Network Map

By default, the following conventions are used in the map window to indicate the status of a device or service:

- **Highlighted device name** — an event has been recorded for the device. For more information, see “Types of Events Logged” on page 104.
- **Green device icon (with a square shaped background)** — the device is “up” (responding to polling)
- **Light green icon (with a diamond shaped background)** — the device has missed at least one polling request
- **Yellow icon (with a diamond shaped background)** — the device has missed two polling requests
- **Red icon (with an elongated diamond shaped background)** — the device is “down” (It is not accessible or has not responded to four consecutive polling requests).

**Note**

After missing 8 polling requests, the background shape becomes a starburst.

- **Purple icon (with an octagon shaped background)** — a standard service on the device is down

You can change the default colors in the map properties, as described in the “Program Options (Map Colors)” topic in Help. You can also change the default device shapes in the map properties, as described in the “Program Options (Device States)” topic in Help.

You can quickly display a brief status message by moving the cursor over a device icon. In the status bar of the map window, a message displays the device’s host name, IP address, and current status or service status.

WhatsUp Gold displays a count-down timer on the right side of the status bar of the map window. The timer is set to the map **Poll Frequency** (Right-click a blank space in the map, select **Properties** and click **General**) and counts down to one between each poll. WhatsUp Gold resets this timer after each poll.
Receiving Alarms

If **Enabled Alerts** (on the **Alerts** dialog box of device properties), is selected, AND if you have added an alert to this dialog box, an alert occurs when a device fails to respond to four (the default) consecutive polling requests. To play an audible alert, you must have a sound card installed on your system. You can set the number of failed poll requests that triggers a sound alert.

To silence an audible alert, click the **Quiet** button in the main toolbar, or from the **Monitor** menu, select **Stop Alarm**.

Receiving Notifications

Enabled notifications are sent when:

- The device fails to respond to the specified number of polling requests
- A monitored service goes down
- An SNMP trap is received for a device

To view the active notifications for a network map, from the **View** menu, select **Notifications**. For more information, see “Viewing Active Notifications” on page 101.

Acknowledging Alerts

To acknowledge alerts, from the **Monitor** menu, select **Acknowledge Pending Alerts**. **Acknowledge Pending Alerts** is active only when there are unacknowledged alerts. Clicking it acknowledges alerts and prevents any pending alerts from being sent.

Using Quick Status (Status)

To display status information associated with any of the displayed devices (active or inactive), right-click the device, select **Quick Status**, and click **Status** to display current status information.
The **Status** dialog box displays the status of packets sent by WhatsUp Gold to poll this device and a current status message. These status numbers are measured from the last time the device’s counters were cleared.

- **Status.** Current status of the device. A zero status code indicates the device is up. A numeric status code above 10000 is a Winsock error code. The text for the error message is also displayed.

- **Count.** Total number of times this device was polled.

- **RTT.** Round Trip Time (RTT) is the time (in milliseconds) that it took the last packet sent to arrive at the device and return.

The **ICMP Status** dialog box shows the following three items for the Device Status and Service Status:

- **Down Count.** Count of how many polls have passed since the device or service last responded.

- **Total.** Total count of how many polls occurred where the device or service did not respond since the counter was last cleared, WhatsUp Gold started, or since the device was added to the map.

- **Last Response Time.** Time of day (in hours:minutes:seconds) of the last response.
The services graph at the bottom of the dialog box shows the status of any services being monitored on the device (as specified on the Services dialog box of device properties). Services cannot be monitored if NetBIOS or IPX is the selected polling method. A service is green if it is up, red if it is down.

You can also display the following status information from within a device’s properties:

- Click **History** (right-click the device, select **Quick Status** and click **History**) to display a graph of the round trip times of the device over the last 30 polls. Red vertical bars indicate the device was not responding.
- Click **Up-Time** (right-click the device, select **Quick Status** and click **Up-Time**) to display a pie chart that shows the percentage of successful polls for the total poll count.
- Click **Log** (right-click the device, select **Quick Status** and click **Log**) to display any service or device “up” or “down” events for this device. On the **Alerts** dialog box, you can select **Enable Logging** for the device (right-click the device, select **Properties**, and then click **Alerts**).

**Using the Status Window**

The Status Window shows a list of all the devices in the currently active map and displays the status using the same colors used on the map. It also shows the status of any services being monitored.

From the **View** menu, select **Status**.

![Status Window Example](image-url)
You can monitor the network through the Status Window. You many need to expand the Status Window in order to read the service status information.

In the main toolbar, click the **Poll** button to start a single check of each device in the Status Window. Click the **Stopwatch** button to start automatic polling of each device.

You can double click a device in the Status window to display the device properties.

### Viewing and Changing Dependencies

By default, WhatsUp Gold polls devices in the order that they were added to the map. In the Dependencies Window, you can view and change the polling sequence and a device’s dependency on other devices.

You can set or change a dependency so that certain devices get polled only if another device that they are connected to is up or down. For example, you may want to poll intervening routers only if the end point cannot be reached. An easy way to set this up is to use the Traceroute tool (see page 181) to automatically map a path to an address and tell it to **Set Dependencies**. Look at the result in the Dependencies Window after doing this.

From the **View** menu, select **Dependencies**.
The Dependencies Window shows the network as a hierarchical tree showing the polling sequence and user-defined up and down dependencies. The value in the parenthesis after the name is an item identifier to resolve ambiguous device names.

Poll Sequence and Up Dependencies. Devices are listed in the order they are polled. If a device is “up dependent” on the device above it, it is indented. You can drag a device within the branch to change the polling order of the device.

To change the polling sequence, do one of the following:

- In the Poll Sequence and Up Dependencies list, drag a device to a different location in the Poll Sequence list.
- Right-click a device and use the popup menu.
- Select a device and use the Move to menu.

The following commands appear on the popup. Move to menu:

Start of Poll. Make the device the first device to be polled.

Move Earlier in Poll. Move the device up one position in the order.

End of Poll. Make the device the last device to be polled.

Later in Poll. Move the device down one position in the order.

Setting “Up” and “Down” Dependencies

You can set any of the devices in the map to have an “up” or “down” dependency on another device in the map. An “up dependency” means that the device is checked only if another specified device is up. A “down dependency” means that the device gets checked only if the other device is down.

Dependencies are shown in the Up Dependencies and Down Dependencies lists by their location and indentation. If a device is dependent on another device, it is indented below the other device.

To set an up or down dependency:

1. In the Up Dependencies or Down Dependencies list, move the device that you want to have a dependency so that it appears just below the device it will depend on.
2. Right-click the device that you want to have the dependency.
3. Select Depend on Prior Device from the right-mouse menu.
Viewing the Polling Statistics

WhatsUp Gold provides easy access to the polling statistics for the active map. From the View menu, select Statistics to view the accumulated statistics for each device in the active network map.

The polling statistics are retained when you close or open network maps. Each map has an associated .wui file. Polling statistics are logged in the map_name.wui file.

<table>
<thead>
<tr>
<th>Device</th>
<th>Address</th>
<th>Type</th>
<th>Status</th>
<th>Period</th>
<th>Down</th>
<th>Rate</th>
<th>Avg</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Statistics Window lists all of the devices in the network map and shows the following statistics for each device:

**Device.** The device name.

**Address.** Device address (if the polling method is ICMP or TCP/IP).

**Type.** The polling method (ICMP, TCP, NetBIOS, or IPX) set on the General dialog box in the device properties.

**Status.** The device’s last read status. A zero status indicates the device is up. Any other value indicates an error. If it is a TCP/IP device, you may see a status code above 10000, a Winsock error code. To view a reported error, right-click the device, select Quick Status, and click Status.

For each device, the Statistics Window also shows the counters described below. These values are cumulative until you reset them for a map in one of two ways:

- Using the **Reset Counters** command on the Monitor menu
  *(available only when the Statistics Window is open)*

- Using the **Reset Counters** function in the web interface

The counters shown in this window are not the same as those shown
in the Statistics Log. Counters in the Statistics Window are cumulative per device. Counters in the Statistics Log are written per device at an interval determined by the setting on the **Logs** dialog box (**Configure**->**Program Options**->**Logging**, then clicking the **Advanced** button).

For information on WhatsUp Gold Syslog, see “WhatsUp Gold Syslog” on page 104.

**Period.** The time (in *hours:minutes*) since the counters were last cleared.

**Count.** The number of times the device has been polled since last cleared.

**% Responded.** Of the total number of polls to the device, the percent that responded.

**% Missed.** Of the total number of polls to the device, the percent that failed.

**Down Time.** The total down time (in *hours:minutes*) for this device. This is calculated by multiplying the number of missed polls by the Map Poll Frequency. For example, if the device misses 7 polls, and the poll frequency is once per minute, the down time will be 7 minutes.

**# Alerts.** The number of alerts that have occurred for the device.

**AvgRTT.** Average round trip time (RTT) of the last polls sent.

**MinRTT.** Minimum RTT of polls sent to the device.

**MaxRTT.** Maximum RTT of polls sent to the device.

You can click any of the column headings to toggle the sort between ascending and descending.
Viewing Active Notifications

You can view the notifications enabled for the active network map.

From the View menu, select Notifications

The notifications are grouped by device. Click a column heading to toggle the sort between ascending and descending order.

Using the Mini Status View

The Mini Status view is a small profile window that you can use to monitor network status in place of the map window. The Mini Status view lists all devices in the currently active maps and displays status using the same colors used in the map window.

From the View menu, select Mini Status Mode. The WhatsUp Gold main window is closed and the Mini Status view appears.

Double-click a device name to view the Alerts dialog box of the device properties.

Each open map is listed in a separate column. Any services being monitored on a device are shown.

Click the Mini Status view to silence an alarm.

Double-click the Mini Status view to close it and go back to the map window.
Chapter 6: Logs and Reports

WhatsUp Gold logs three types of data:

- **Events** — Events are changes to network status, such as a device going down or a device coming back up. Events are recorded in the Event Log (EV-yyyy-mm-dd.tab), which provides a history of what has occurred on the network. In addition, the Debug Log window provides a view of events as they occur.

- **Polling statistics** — Polling statistics are the accumulated round trip times (RTT) of polls sent to a device. These statistics measure the availability and performance of a device. Polling statistics are recorded in the Statistics Log (ST-yyyy-mm-dd.tab).

- **SNMP traps** — The SNMP Trap Log displays all SNMP traps that have been received. When using this viewer, all traps can be seen (unlike using "Quick Status" on a device, which filters explicitly for individual traps for that device). To enable SNMP traps, go to Configure->Program Options->SNMP Traps and select Enable SNMP trap handler.

From this logged data, WhatsUp Gold can create several reports and graphs that show the status of your network in different ways. From the Reports menu, you can create the following:

**Performance Graphs.** Show devices by best or worst performance based on aggregated polling statistics, and shows graphs for each device.

**Event Reports.** Show device up and down events, service up and down events, and WhatsUp Gold events such as map open and close. You can print this report or create a tab-delimited file from it.

**Statistics Reports.** Show round trip times and percentage of missed polls based on the accumulated polling statistics for each device. You can print this report or create a tab-delimited file from it.

---

**Note**

Performance graphs are not available from the web interface, but can be exported to HTML format (for more information, see “Using the Command Line for Performance Graphs” on page 128.).
**WhatsUp Gold Syslog**

What is a Syslog?

WhatsUp Gold’s Syslog Daemon receives standard UDP messages sent from routers, switches, UNIX hosts, or any device that can generate UDP network traffic. Once a message is received, the Syslog logs the message to disk along with a timestamp and the IP Address of the device originating the message. The Syslog stores its data in weekly file increments with the same file name format as the other log type systems within WhatsUp Gold: ‘SL-YYYY-MM-DD.tab’.

For more information refer to the help file: “WhatsUp Gold Syslog”.

---

**Logging and Reporting Events**

WhatsUp Gold logs events in the Event Log (EV-yyyy-mm-dd.tab) and lets you create reports based on the event data.

WhatsUp Gold automatically logs application-level events (such as opening or closing a map) and device-specific events (such as a device or service down) for devices that have **Enable Logging** selected on the **Alerts** dialog box. After WhatsUp Gold logs sufficient event data, you can generate reports on the data or save the data in a tab-delimited format that can be imported to another application.

The following sections describe the types of events logged, how you can modify event logging, and how you can generate reports on the events.

**Types of Events Logged**

WhatsUp Gold records events in the log (EV-yyyy-mm-dd.tab) as they occur. WhatsUp Gold logs the following types of events for any open maps:

- Map changes — includes map open and close and changes to the map configuration.
- SNMP traps — logs SNMP trap server start or stop and any SNMP traps received for a device.
• Device changes — for devices that have **Enable Logging** selected on the **Alerts** dialog box, WhatsUp Gold logs an up or down alert for a device or a service and missed polls for a device. When a device comes back up, it logs the total number of missed polls and the total down time.

• Notifications — all notifications that get sent are logged.

• Acknowledged Alerts — logs an event when you select **Monitor** > **Acknowledge Pending Alerts** (to clear all alerts) on the console or click **Acknowledge** in the web interface.

• Access table lockout events — occurs when a web access attempt is denied, for example, due to settings in the **IP Security**. *(Configure->Web Server->IP Security)* The log entry also shows the IP address of the host that attempted to log on to the web server.

• NT Service events — any up or down events resulting from checking an NT Service.

### Changing How Events Are Logged

The application-level events (such as opening or closing a map) are logged automatically. For device-specific events, you can specify:

- Whether the up or down events for a device are logged
- The number of polls missed (**Threshold**) before a “DOWN” or “SVSDOWN” event is recorded for a device or for a monitored service on a device

**To change how events are logged for a single device:**

1. Right-click the device and select **Properties**.
2. Click **Alerts**.
3. To log “UP” and “DOWN” events for this device, make sure **Enable Logging** is selected. (These entries can be viewed by right-clicking the device and selecting **Quick Status**, then clicking **Log**.)

The **Logging Trigger** default value is 1, which means that every missed poll is logged; this setting gives you the most complete information about your network: when a device (or a monitored service on the device) misses one poll, it is logged as “DOWN” or “SVCDOWN.” We recommend that this number be at least 4.
If you have a device on your network that routinely misses just one poll, you may feel that you are getting too many “Down” or “Up” messages in the Event Log. In this type of situation, you can set the Trigger to a higher number such as 2, 3, or 4. To find the Trigger value, select the alert and click the Edit button.

However, if you have assigned notifications to this device and want to make sure, for clarity’s sake, that a “Down” or “Up” event for this device is recorded in the Event Log before any alerts or notifications are recorded, make sure the Trigger value is less than or equal to the Logging Trigger value of any notifications assigned to this device.

4 Click OK to save your changes.

To change how events are logged for all devices or multiple selected devices:

1 (Optional) To change how events are logged for multiple devices in the map, select the devices.

   Note

   To select multiple devices, hold down the Ctrl key and click the desired devices.

2 Right-click one of the selected devices and select Add Alerts to Group. The Add Alerts To Group displays a special property sheet that contains only “Alerts” and “Menu” pages. When in this setting, every alert you add is added to all the devices that are currently selected. This makes it quite easy to add the same alert on multiple devices.

3 The rest of the steps are identical to the previous page.
Viewing the Event Log

The Event Log provides a history of the events that occur for any network maps that are open. For a description of the events that get logged, see “Types of Events Logged” on page 104.

To view the event information, from the Logs menu, select Event Log. The following screen shows an example:

The Event Log shows the date and time an event occurred, the type of event, and other pertinent information depending on the type of event.

The Event Log holds the event data for all of your WhatsUp Gold maps. It holds data starting with either the date you first started monitoring a map or the date since log management last performed its cleanup. For as long as any map is open, all related map events are recorded in the Event Log, including devices and services going down, devices or services coming back up after being down, and alert acknowledgements. The Event Log also records SNMP traps (if the SNMP trap handler is enabled) and denials of web access; these types of events are recorded any time WhatsUp Gold is running, even if no maps are open.

Log Viewer: This is the viewing screen where a user can view existing logs. The viewing mechanism displays in weekly increments. The view defaults to the current week. The date of the currently viewed week is displayed at the top of the dialog box.

Back icon: The ‘Back’ icon displays the past week’s log.

Current icon: The ‘Current’ icon displays the current accumulating log for that week.
**Forward icon:** The ‘Forward icon is grayed unless a user selects the ‘Back’ icon, so that the user has the functionality to sift back and forth between multiple accumulated weeks worth of log files.

**Find icon:** The ‘Find’ icon launches a small dialog box used for finding text in the display.

**Filter icon:** The ‘Filter’ icon launches a filter dialog box, which allows the user to customize the log viewer so that they can see their logs in a different time span other than weekly. This dialog appears when you click the Filter icon and change a filter from an “off” state into an “on” state. Once you click the OK button on this dialog, focus will return back to the Log Viewer and the Filter icon will be pushed in, representing the fact that a filter is in place. Clicking the Filter icon again (or the menu equivalent) causes the filter icon to be pushed out (decompressed) which represents the fact that no filter is in place. When a filter is in place, the "Back" and "Forward" buttons on the Log Viewer confines the browsing ability to the dates specified in the filter.

---

**Note**

A common misconception is that all the data for the range specified is displayed at once, this is not correct, the "Back" and "Forward" buttons are still used to display the filtered data in weekly increments

---

You can either specify your time period in **Week(s)**, **Month(s)**, **Year(s)**, or you can select a **Range**.

- If you select **Week(s)**, you must specify how many weeks back you want to include. Example: Selecting 1 week will display information from the current date back to seven days prior.

- If you select **Month(s)**, you must specify how many months back you want to include. Example: Selecting 1 month will display information from the current date back to four weeks prior.
If you select Year(s), you must specify how many years back you want to include. Example: Selecting 1 year will display information from the current date back to fifty-two weeks prior.

If you select Range, you must specify the starting and ending dates.

Refresh icon: The ‘Refresh’ icon allows for the viewer to be updated with messages that have been logged since initially opening the log file.

Print icon: When the log viewer is opened, the ‘Print’ icon will appear (or be enabled) on the ‘File’ menu to allow a user to print the contents of the log viewer.

Format option buttons: The ‘Raw’ and ‘Formatted’ buttons provide two options. The ‘Raw’ layout is a display with no columns, and just a listing layout. In ‘Raw’ format, the user has the ability to cut & paste their data to an outside source. The ‘Formatted’ layout inserts the data into columns and formats the date and time to be human readable.

Creating an Event Report

After WhatsUp Gold has been monitoring a map long enough to generate event data, you can create reports based on the event data. For a description of the events that get logged, see “Types of Events Logged” on page 104. If you want to change how events get logged, see “Changing How Events Are Logged” on page 105.

To create an Event Report:


2. Select the Map Name of the map for which you want a report.

3. Select the Report Type.

Event Report dialog box
**Summary.** Reports total service and device down time for each device and sorts by device name in Ascending or Descending order. You can also sort by Worst First order, which means the device with the most down time is shown first.

**Detail.** Reports all up and down events for each device. For each device down event, the elapsed down time is reported. The report sorts devices by device name in Ascending or Descending order. You can also sort by Worst First order, which means the device with the most down time is shown first.

In addition, the Detail report shows the following events: map configuration changes, acknowledge alerts events, NT service restarts, and access table lockouts. For more information about these events, see “Types of Events Logged” on page 104.

**Raw Data.** Exports the data from the Event Log to a tab-delimited file that can be imported to another application. The data is sorted by date and time in ascending order.

4 Select the **Date Range** for the report.

When you select an option, the Start Date and End Date are shown.

The default includes all days since you started monitoring the map, or since the event data was last cleared by clicking Clear in the Event Log or by clearing the log from the web interface.
5 Click OK to generate the report.

WhatsUp Gold generates the specified report and displays it in the Report Window. From the Report Window, you can save the data to a file, print it, or copy data to another application.

![Report Window]

**Note**

If you get the message “insufficient data,” it’s possible that you have not monitored the map long enough to generate event data.

**Debug Log Information**

All actions, such as poll requests and service checks performed by WhatsUp Gold, are shown in the Debug Log window. The Debug Log is a real-time log that displays WhatsUp Gold events as they occur. To view the log, from the Logs menu, select **Debug Log**.
Using the Command Line for Event Reports

`Wugrpt.exe` is a utility that can generate reports from the Event Log (`EV-yyyy-mm-dd.tab`) data. You can invoke `wugrpt` from the Windows Command Prompt (MS-DOS prompt). By default, the report is displayed in the Command Prompt or MS-DOS window.

**Basic Command Syntax**

```
wugrpt -m mapname [-s yyyy-mm-dd] [-e yyyy-mm-dd] [-l logfile] [-osortmode] [-r report] [-t maptitle]
```

**Note**

You must use the `-m` argument to specify the name of the WhatsUp Gold map to use for the report. All other arguments are optional.
### Examples

The following examples create Event Reports for the *Boston1* map:

- `wugrpt -m "C:\Program Files\Whatsup\network1.wup"`  
  Generates a detail report for all days in the log (uses defaults).

- `wugrpt -m "C:\Program Files\Whatsup\Boston1.wup" -s 20010301 -e 20010331`  
  Generates a detail report for one month of log data.

### Return Codes

`Wugrpt` returns 1 if it performed at least one of the requested operations; it returns 0 if it failed.
Logging and Reporting Polling Statistics

WhatsUp Gold lets you log and report on polling statistics to provide a picture of how your network is performing over a selected time interval.

WhatsUp Gold can log polling statistics for each device in an open map. After WhatsUp Gold logs sufficient polling data, you can generate reports on the data, create performance graphs, or save the data to a tab-delimited file that can be imported to another application.

The following sections describe the polling statistics, how you can change statistics logging, and how you can generate reports from the statistics. For information on performance graphs, see “Creating Performance Graphs” on page 121.

The Polling Statistics

WhatsUp Gold writes values for the polling statistics to the Statistics Log (ST-yyyy-mm-dd.tab). By default, the statistics data is saved to the log every hour, but you can change this interval.

WhatsUp Gold can log the following polling statistics for each device in an open map:

**Average RTT.** The average Round Trip Time (RTT) for polls to the device. This average is taken over the interval you specify for statistics generation. See “Changing Statistics Logging” on page 115. The default value is one hour.

**Maximum RTT.** The highest RTT recorded for the device during the statistics interval (default is one hour).

**Minimum RTT.** The lowest RTT recorded during the statistics interval (default is one hour).

**Percentage of missed polls.** The average percentage of missed polls during the statistics interval (default is one hour).

Note that the counters shown in the Statistics Log are not the same as those shown in the Statistics Window. Counters in the Statistics Window are cumulative per device. Counters in the Statistics Log are written per device at an interval determined by the setting on the Logging dialog box of program options (Configure->Program Options->Logging, then click the Advanced button.)
Changing Statistics Logging

You can set how often you want polling data written to the Statistics log (ST-yyyy-mm-dd.tab). By default, statistics are written every hour.

To set how often to update the Statistics log:

1. From the Configure menu, select Program Options and click Logging.
2. In the Log type list box, select “Whatsup Statistics”
3. Click the Advanced button
4. In Log update interval, change the value for hours. You can set this value from 0 to 254 hours. To turn off statistics logging, set the value to zero.
5. Optionally, click Update Log to write current statistics to the log and reset the counters for each statistic.

Creating Reports on Polling Statistics

After WhatsUp Gold has monitored a map long enough to generate statistics data, you can create reports based on the statistics.

To create a statistics report:

2. Select the Map Name of the map for which you want a report.
3. Select the Report Type.

Detail. Report polling statistics for each device and sort by device name in Ascending or Descending order. The reported statistics are calculated from data in the Statistics Log. For definitions of the reported statistics, see “Statistics Report Legend” on page 117.
**Raw Data.** Save the data from the Statistics Log to a tab-delimited format that can be imported by another application. The data is sorted by device polling order. See “Exporting Raw Data” on page 117.

**Day of the Week.** For each day of the week, it reports all up and down events for each device. For each device down event, the elapsed down time is reported.

4 Select the **Date Range** for the report. When you select an option, the **Start Date** and **End Date** are shown.

5 Click **OK** to generate the report.

WhatsUp Gold generates the specified report and displays it in the report window. From the report window, you can save the data to a file, print it, or copy data to another application.

---

**Note**

If you get the message “insufficient data,” it’s possible that you have not monitored the map long enough to generate polling statistics.
Exporting Raw Data

As mentioned above, you can create a raw data file of the Statistics Report. The tab-delimited raw data file can be imported by another application, for example by a spreadsheet application.

Statistics Report Legend

The values in the statistics report are calculated from the data in the Statistics Log (ST:yyyy-mm-dd.tab). When you create a statistics report, WhatsUp Gold calculates the average daily values for each device in the selected map; the average daily values are based on the number of data samples in the Statistics Log. Thus, the report shows:

Sample. Number (n) of data samples used to calculate the averages. If you use the default for statistics generation (one hour), then if the map was monitored for all 24 hours of the day, you will have 24 samples.

Average RTT. The arithmetic mean of n samples of Round Trip Time (RTT).

Average Maximum RTT. The arithmetic mean of n samples of Maximum RTT.

Average Standard Deviation. The standard deviation of the RTT values.

Average Minimum RTT. The arithmetic mean of n samples of Minimum RTT.

Average Percentage of Missed Polls. The arithmetic mean of n samples of the percentage of missed polls.
Using the Command Line for Statistics Reports

Wugstat.exe is a WhatsUp Gold utility used to generate reports from WhatsUp Gold Statistics Log (ST-yyyy-mm-dd.tab) data.

You can invoke wugstat from the Command Prompt or MS-DOS prompt. You must invoke wugstat with the -mmapname argument. All other arguments are optional. By default, the report is displayed in the Command Prompt or MS-DOS window.

Basic Command Syntax

You must use the -m argument to specify the name of the WhatsUp Gold map to use for the report. All other arguments are optional.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m mapname</td>
<td>Optional. The name of the map to use as the basis for the report. Can be a regular expression search string such as: local.*</td>
</tr>
<tr>
<td>-s yyyyMMdd</td>
<td>Optional. Start date to use as the basis for the report. Use -s to specify the start date for the report. The default is the oldest date in the log.</td>
</tr>
<tr>
<td>-d devicename</td>
<td>Optional. The name of the device to use as the basis for the report. Can be a regular expression search string such as: router.*</td>
</tr>
<tr>
<td>-e yyyyMMdd</td>
<td>Optional. End date to use as the basis for the report. Use -e to specify the end date for the report. The default is the most recent date in the log.</td>
</tr>
<tr>
<td>-l logfile</td>
<td>Optional. Argument used to specify an alternate log file. Use -l to specify an alternate log file. The default is wugstatdata.tab.</td>
</tr>
<tr>
<td>-o sortmode</td>
<td>Optional sort order. Valid values for sort mode are: ascend (sort by device name in ascending order), and descend (sort by device name in descending order). Use -o to specify one of the sort modes: Ascend sorts by device name in ascending order (this is the default value); Descend sorts by device name in descending order</td>
</tr>
<tr>
<td>-r report</td>
<td>Optional. Name of report to generate (default detail report). Valid values for report are: detail (generates a detailed summary report by device), dow (generates a Day of the Week detailed report by device), and export (generates a tab delimited output file of raw data). Use -r to specify one of the report types:</td>
</tr>
<tr>
<td>-t maptitle</td>
<td>Optional, the title to use at the top of the report. Use -t to specify the title to use at the top of the report. The default title is the map name.</td>
</tr>
<tr>
<td>-?</td>
<td>Use -? to see a summary of argument options.</td>
</tr>
</tbody>
</table>
Examples
The following examples create statistics reports for the Boston1 map:

wugstat -m Boston1.wup

generates a detail report for all days in the log (uses defaults).

wugstat -m Boston1.wup -s 20010301 -e 20010331

generates a detail report for one month of log data.

Return Codes

Wugstat returns 1 if it performed at least one of the requested operations; it returns 0 if it failed.
Creating Performance Graphs

You can graph the polling statistics that WhatsUp Gold accumulates for the devices on your network. The graphs show performance for a device by plotting the average time it takes a device to respond to a poll, known as the round trip time (RTT). In addition, the Performance Graphs can show aggregate data, such as the devices with the best and worst availability, or the devices with the highest and lowest average missed polls, and the best and worst days of the week for network performance.

High values for response time (RTT) indicate poor performance, low values indicate good performance, and low values for missed polls indicate high availability.

Graphs are based on data in the ST-yyyy-mm-dd.tab. For information about this log, see “Logging and Reporting Polling Statistics” on page 114.

Note

If Performance Graphs in the Reports menu is grayed out, you need to install Microsoft’s ODBC and the ODBC text driver. To install ODBC, see “System Requirements” on page 6.

Graph Options

When you create a Performance Graph, you can choose:

• the time interval for which you want to see statistics: daily, weekly, monthly, or all observations in the log
• in some cases, the graph format: bar chart or area chart
• how you want to sort the data: by device name; in ascending or descending order
• which maps and which devices to include in a graph

All graphs show both aggregate performance data for the selected time period and the data for each device.
Creating a Graph

To create a graph:

1. Start the Performance Graphs tool by doing one of the following:
   - From the Reports menu, select Performance Graphs.
   - From the Start menu, select WhatsUp->WhatsUp Gold->WhatsUp Gold Performance Graphs.

   The WhatsUp Gold Performance Graphs dialog box appears.

   2. Select the Report Type to set which performance data you will view and the format of the graph. To see examples of graphs, see “Sample Performance Graphs” on page 126.

   **Comprehensive Report.** Shows devices by average response time for the selected period. This includes slowest devices; slowest dates for overall response time (all devices); and slowest days of the week for overall response time (all devices). Within the report, you can select a device to show its own graph.

   **Daily (Line Chart).** Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by date recorded. Within the report, you can select a device to show its own graph.
**Day of the Week (Area Chart or Bar Chart).** Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by the day of the week. For example, the averages for Monday, the averages for Tuesday, etc. This graph can be shown as an Area Chart or Bar Chart. Within the report, you can select a device to show its own graph.

**Monthly (Area Chart or Bar Chart).** Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by month. For example, the averages for January, the averages for February, etc. This graph can be shown as an Area Chart or Bar Chart. Within the report, you can select a device to show its own graph.

**Daily Text Report.** Shows a daily average for each of the statistics per device. You can select the devices and the period for which you want to display data.

**Availability Report.** Shows the availability of devices based on average missed polls. This includes the best and worst availability over the selected period; best and worst dates for overall availability (all devices); best days of the week for overall availability (all devices). Within the report, you can select a device to show its own graph.

**Wugstathour.rpt.** Shows an hourly performance report.

3 Select the **Date Range** for the report. When you select an option, the **Start Date** and **End Date** are shown.

The default includes all days since you started monitoring the map, or since the statistics were last cleared by clicking **Clear** in the Statistics Log or by clearing the log from the web interface.

Select **Custom** if you want to enter a **Start Date** and **End Date** for the report. Enter dates in the format yyyymmdd, for example: 20000208.

4 The **Data Source** box shows **wugstatdata.tab** as the default value. Current statistics are always logged to **ST-yyyy-mm-dd.tab**. To archive statistics, you can copy the current statistics to a different file name — as long as the file is in the WhatsUp top directory and its name starts with **wugstats**, it will appear in the **Data Source** list box.
5 The **Sort Field** box shows that the performance data is sorted by the device name, in alphabetical order. You can select to sort in **Ascending** or **Descending** order for all reports (except the Comprehensive Report).

6 Enter the Report Selection Criteria to determine which maps and which devices to include in the graph.

The default values graph performance data for all maps and all devices for which there is data in *ST-yyyy-mm-dd.tab*. You can change the criteria to graph performance data for any combination of maps and devices.

**MapName.** Use *All maps* to graph all data. To choose from a list of your maps, select contains, and then select a map name from the **Search String** box. You can also select the search expression (such as contains, starts with), and then enter the search text (such as a map name or partial map name) in the **Search String** box. (See “Using Search Expressions” below.)

**DeviceName.** Select *All devices* or select the search expression (such as contains, starts with), and then enter the search text (such as a device name or partial device name) in the box to the right. (See “Using Search Expressions” below.)

7 Use **Zoom Factor** to change the view size of the report.

8 Click **Create Report.** You may have to wait a few seconds for the report to appear, depending on the number of devices included in the report. For examples of graphs, see “Sample Performance Graphs” on page 126.
Using Search Expressions

When setting criteria for which maps and devices to include in a report, you can specify a search expression accompanied by search text.

The following table lists the search expressions you can use:

<table>
<thead>
<tr>
<th>Search String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all maps or all devices</td>
<td>Include all maps or all devices</td>
</tr>
<tr>
<td>contains</td>
<td>Include maps (or devices) that contain the search string; or select a map from the list box in the Search String box. ? = one character; * = many characters</td>
</tr>
<tr>
<td>does not contain</td>
<td>Exclude maps (or devices) that contain the search string</td>
</tr>
<tr>
<td>starts with</td>
<td>Include maps (or devices) that start with the search text</td>
</tr>
<tr>
<td>does not start with</td>
<td>Exclude maps (or devices) that start with the search text</td>
</tr>
</tbody>
</table>

**Search String.** To enter the Search String, enter the literal text that you want to search for. For example, if you want to report on a device named wks120, type: wks120. To simplify selection of a map, us the "*" for example: *whatsup1.wup will match C:\Program Files\WhatsUp\whatsup1.wup.

---

**Note**

The "contains" and "does not contain" search expressions are not case sensitive.

---

If you use the contains expression, you can use ? or * in the Search String. For example:

wks? -finds wks1, wks2, wks9; but does not find wks10, or wks120

wks* finds wks1, wks10, and wks120
Sample Performance Graphs

The following example shows a Comprehensive Report for all devices in a map.

Click a device name to view its graph.

Gyro was the slowest device.

The network was slowest on 1999 11 10.
You can click a device name in the left panel to see the graph for that device, as shown in the following example.

**Viewing, Printing, and Exporting Performance Graphs**

When you create a performance graph, it appears in the graph viewer. If there are graphs of the aggregated values for all devices, these graphs appear on the first pages of the report. The remaining pages of the report show graphs of individual devices. The exception is the Daily Text Report, which shows formatted text and does not contain graphs.

**Device list.** The left frame of the report viewer lists the devices in the report, by host name or IP address. To display the graph for a device, click on a device in the left frame.
**Tool Bar.** Use the buttons in the tool bar to navigate or print the report, export report data to another format, or change the report display.

**Printing Graphs**

To print a graph, click the **Print** icon in the tool bar and enter your print options. To change the default printer, click the **Print Setup** icon in the toolbar.

**Exporting Graphs**

You can export the currently displayed graph to a variety of formats, including HTML. To export a graph:

1. Click the **Export** icon in the toolbar. The Export dialog box appears.
2. Select a **Format**. Select HTML, text, RTF, or a specific application’s format.
3. Select a **Destination**.
4. Click **OK**.

You can view the exported graph in a tool that supports the selected format.

---

**Using the Command Line for Performance Graphs**

*Cstatrpt.exe* is a WhatsUp Gold utility that can generate Performance Graphs from the Statistics Log (ST-yyyy-mm-dd.tab files) data. You can invoke cstatrpt from the Windows Command Prompt (MS-DOS prompt). By default, the report is displayed in the Performance Graphs interface. The `-x` (for Export) argument is the only non-interactive mode (meaning no dialog boxes are displayed). The `-x` option creates a Performance Graph in HTML format, which you can display in a browser.
### Basic Command Syntax


<table>
<thead>
<tr>
<th>Argument</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m mapname</td>
<td>The mapname must include the full path. For example, cstatrpt -m C:\Program Files\whatsup\network1.wup. You can enter a complete map name, or enter a partial name. For example, -m network will include network1, network2, network3 etc.</td>
</tr>
<tr>
<td>-d devicename</td>
<td>Use -d to specify the name of a device on which to base the report. You can enter a complete device name, or a partial name to include all devices that match the partial name. For example -d WKS will include WKS1, WKS2, WKS3 etc.</td>
</tr>
<tr>
<td>-D dateopt</td>
<td>Use -D to specify a recurring time period. wtd - Current week to date td - Today lastw - Last week mtd - Month to date lastm - Last month</td>
</tr>
<tr>
<td>-s yyyyymmdd</td>
<td>Use -s to specify the start date for the report. The default is the oldest date in the log.</td>
</tr>
<tr>
<td>-e yyyyymmdd</td>
<td>Use -e to specify the end date for the report. The default is the most recent date in the log.</td>
</tr>
<tr>
<td>-l logfile</td>
<td>Use -l to specify an alternate log file. The default is wugstatdata.tab.</td>
</tr>
<tr>
<td>-o sortmode</td>
<td>Use -o to specify one of the sort modes: Ascend sorts by device name in ascending order (this is the default value); Descend sorts by device name in descending order.</td>
</tr>
</tbody>
</table>

**Logs and Reports**

---

**WhatsUp Gold**
Examples

The following examples create performance graphs for the Boston1 map:

Example 1.

```cstatrpt -m*Boston1.wup```

generates a Comprehensive report for all devices in the Boston1 map for all days in the log (uses defaults, except for the map name).

Example 2.

```cstatrpt -m*Boston1.wup -rwugstatdaily.rpt -Dlastm -x```

generates a daily report for all devices in the Boston1 map using the last month of log data, and exports the graphs to HTML format (does not display the Performance Graphs interface).

Sending Recurring Notifications

A recurring notification is one that is sent at a specified time interval via a pager, e-mail, or beeper notification. A recurring notification contains one or more of the following:

- The count and names of devices that are up
- The count and names of devices that are down
- Names of devices that have a service down
- The most recent lines from the Event Log

You can set options to send the report at a specified interval. This report lets you receive up-to-date status reports at a remote site, so you can be assured the network is running smoothly, or so you can be quickly apprised of any problems.

The following example shows a Recurring Report sent via e-mail:

**Example:**

```cstatrpt -m*Boston1.wup -rwugstatdaily.rpt -Dlastm -x```

This command generates a daily report for all devices in the Boston1 map using the last month of log data, and exports the graphs to HTML format (does not display the Performance Graphs interface).
To set up a Recurring Notification:

1. From the **Configure** menu, select **Recurring Notifications**. The Recurring Notifications dialog box appears.

2. Select **Enable Recurring Notifications**.

   You see the following dialog box:
3 Click **Add**. The Add/Edit WhatsUp Reports dialog box appears.

4 Select a notification from the list box.

5 Enter how often (in minutes) you want to send the report.

6 Select the Time Period when you would like to receive the notification. Click **Change** to change the default setting of 7 days a week, 24 hours a day.

7 Click **OK**.
Chapter 7: Working from a Web Browser

This chapter describes how to set up the WhatsUp Gold web server and use a web browser to access mapping, monitoring, and notification functions from a remote computer.

Setting Up the WhatsUp Gold Web Server

WhatsUp Gold provides a web server that lets you use any web browser on any computer on the Internet to view the status of your network and change WhatsUp Gold settings. You can enable/disable the web server and set access to this server through the web properties. If you run WhatsUp Gold as a Windows NT service (see “Running WhatsUp Gold as an NT Service” on page 11), the web browser will be your primary interface.

To set up the web server:

1. From the Configure menu, select Web Server, and click General to display the setup properties.

2. Select Enable Web Server.

3. If you want web users to be able to change WhatsUp Gold settings from the web interface, select Enable Web Configuration.
You can set access for each web user account (see “Setting Web Access” in this chapter). If Enable Web Configuration is not selected, the web users cannot change any WhatsUp Gold settings; they can use only the view functions.

4 There are two formats for displaying maps in a web browser: Graphical maps, which use JPEG format to display the same icons and colors as maps on the console; or a Text listing of devices in a map. To view the Graphical maps, select Enable Graphical Maps.

5 Enter or change any of the setup information.

   **Main Title.** The title displayed on the main web page (“Top View”) for the WhatsUp Gold web site. You can enter any text for the title.

   **Refresh Frequency.** The number of seconds between updates to the WhatsUp Gold display on the web site. You can set the refresh rate in the range from 10 to 99999 seconds.

   **TCP Port.** The default is port 80, which is the standard TCP/IP port for a web (HTTP) server. If you already have a web server running on this system, set the port number in this box to another port number (for example, 8000).

   **HTML Files Directory.** The default is the \web subdirectory of the directory in which you installed WhatsUp Gold. If you want the WhatsUp Gold web server to serve your own web pages, you can add HTML files to this directory. If you use a different directory, you need to specify the full path in this box. Subdirectories are supported. Note that you should not place a file named default.htm in this directory because WhatsUp Gold uses this name to activate the web server.

   **Map Directory:** This shows the directory path of the map being used.

   **Main Page Prefix.** Enter a message to be displayed at the top of the main web page (“Top View”). You can enter up to 100 characters of plain text and/or raw HTML code in this edit box. The HTML begin and end tags (<HTML> and </HTML>) are automatically added to any HTML code you enter.
**Main Page Suffix.** Enter a message to be displayed at the bottom of the main web page ("Top View"). You can enter up to 100 characters of plain text and/or raw HTML code in this edit box. The HTML begin and end tags (<HTML> and </HTML>) are automatically added to any HTML code you enter.

---

**Note**
Within the Main Page Prefix or Suffix, you can create a link to other web pages. These web pages must be installed in the HTML Files Directory.

---

6 Click **OK** to apply your changes. The changes take effect immediately.

**Customizing Your WhatsUp Gold Web Site**

The following example shows the main web page with prefix and suffix information displayed:
Making Maps Available for Web Viewing

Any network maps that are open in WhatsUp Gold can be viewed from a web browser. In addition, web users with Configure program permission can load any maps in the map directory on the system where WhatsUp Gold is installed. There are two ways to set the map directory:

- From the WhatsUp Gold console, in the Configure menu, select Web Server, click General to display the Web Server Properties. In the Map Directory box, enter the full path for the directory that contains the network maps.
- From a web browser, log on to the WhatsUp Gold web server. The web site main page (“Top View”) appears. Select Settings to display the program settings. In the Startup Map Directory box, enter the path for the directory that contains the network maps.

You must restart WhatsUp Gold for the change to take effect.

Setting Web Server Access

There are two ways that you can set access to the web server. You can use either one or both together:

- Require a user ID and password to view page on the WhatsUp Gold web site. This includes setting the pages and functions that the user can access.
- Specify an IP address or set of IP addresses that are either granted access to the web site or are denied access.

Default User Accounts for the Web Server

WhatsUp Gold provides two default user IDs for accessing the web server: Both of these default user IDs can be deleted if you wish.

- The user ID admin (which has a password of admin) has full access to WhatsUp Gold views and functions, (they can set up or change web user accounts).
- The user ID guest (which has no password) has access to all WhatsUp Gold views but cannot change any WhatsUp Gold settings. If you do not want users to access the web server in this way, then you should disable the privileges for the guest account.
Setting Up User Accounts for the Web Server

You can add an unlimited amount of user accounts for web access to WhatsUp Gold and you can assign different levels of access to each user.

1 From the Configure menu, select Web Server and click Users to display the user access properties.

2 Select the Enable Web Security option (make sure it is checked). If this option is not selected, web users can log on without specifying a user ID or password.

3 Click the Add User button.

4 The Add User dialog box appears and displays all available maps that you can assign to your user.

5 In the Username text box, enter the desired username. This is case sensitive and may contain up to 39 characters.

6 In the Password text box, enter the desired password. This is case sensitive and may contain up to 39 characters.

7 All of the maps are listed in the Available Maps column. Using your mouse, select the map(s) you want to make available to this user. You can select multiple maps by simply clicking on each map you wish to select.
Default Map is one of the maps available to the web user(s). If you wanted the user(s) to have the same access to all current and future maps, all you need to do is assign Default Map to the user(s), and select the Map Level Security Settings you want for this user. This will give the user the same rights for ALL maps (current and future). If you wanted different settings for a certain map, then ALSO assign this map to this web user and select the Map Level Security Settings for this map. These settings for this map will override the default map settings (for this map only). Simply put, assigning Default Map to a web user gives them access to ALL maps (current and future) and keeps you from having to enter the same Map Level Security Settings for each and every map. If you do not want the web user to have access to ALL maps (current and future), you will not want to assign Default Map to this web user.

8 Click on the right arrow button (>) to move the selected map(s) to the Selected Maps column. The double arrow buttons (>> and <<) will move all maps back and forth between the Available Maps and Selected Maps columns (without having to select any of them).

9 After you are satisfied with the username, password, and the available maps for this user, click OK. If you want to delete a user, click on the desired user in the Users text box, and press the “delete” key on the keyboard.

10 Select the WhatsUp Gold web functions that you want to provide the user.

---

**Note**

For more information about the WhatsUp Gold views and functions available from the web server, see “WhatsUp Gold Web Display” on page 143.

**Configure Program.** Lets the user change program settings, create a new map, load and unload maps, and create, edit, and assign notifications.

**Configure Users.** Lets the user add, edit, and delete web user accounts.
**Configure Reports.** Lets the user add, edit, and delete report notifications.

**Access Tools.** Lets the user access and use the Ping and Traceroute tools.

**Access Log.** The user can view the log of WhatsUp Gold events.

**Selecting Map Level Security Settings**

Follow these steps:

1. Notice that your created username is shown in the Users text box.
2. Click the plus sign (+) beside the user to display all map(s) assigned to this user.
3. Click on a map and select the **Map Level Security Settings** you want to provide the user.

**Access Host Pages.** The user can click a device name (in the map page) to view a detailed summary of activity for that device. When this option is not selected, you cannot give the user access to the **Configure Devices** function.

**Acknowledge Alerts.** Lets the user acknowledge a change and stop further alerts for the device(s).

**Configure Map.** Lets the user change map settings, reset counters for all devices, and add and remove devices.

**Configure Devices.** Lets the user change host settings; reset counters for individual devices; configure service monitoring; and add, edit, and remove alerts.

4. Individually set the **Map Level Security Settings** for each map assigned to the user.

5. If you want changes made from the web interface (by any web users) to be saved in the WhatsUp Gold application, select **Automatically save changes to users from web interface.** If this option is not turned on, any changes made from the web interface will last only for the duration of the web session.

6. Click **OK** to save your changes.
When a user opens the WhatsUp Gold web pages, they will be prompted to enter the logon user ID and password before they can view the pages.

**Note**
You can disable access to the configuration functions for all WhatsUp Gold web users, thus overriding the settings for each individual user. To do this, from the **Configure** menu, select **Web Server**, click **General**, and then clear the **Enable Web Configuration** option.

**Setting Web Access by IP Address**

You can specify a list of IP addresses to be granted or denied access to the WhatsUp Gold web pages.

To deny access to a specific computer or group of computers:

1. From the **Configure** menu, select **Web Server** and click **IP Security** to display the access properties.

2. Select **Granted Access**.

3. Click **Add**. The “Deny Access On” dialog box appears.
To deny access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you enter 156.21.50.0 and a subnet mask of 255.255.255.0, all IP addresses in the range 156.21.50.1 through 156.21.1.254 will be denied access.

4 Click **OK** to add the IP address(es) to the list. Access will be granted to all computers except those listed.

5 In the **IP Security** dialog box, click **OK** to save the changes.

*To grant access to a specific computer or group of computers:*  

1 In the **IP Security** dialog box, select **Denied Access**.

2 Click **Add**. The “Grant Access On” dialog box appears.

   To grant access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you enter 156.21.50.0 and a subnet mask of 255.255.255.0, all IP addresses in the range 156.21.50.1 through 156.21.1.254 will be denied access.

3 Click **OK** to add the IP address(es) to the list. Access will be denied to all computers except those listed.

4 In the **IP Security** dialog box, click **OK** to save the changes.

If the **Enable Web Security** option (in the **Users** dialog box) is selected, when a user logs on from a valid IP address, they are prompted to enter the logon user ID and password before they can view the specified pages.

In the **IP Security** dialog box, to edit a web access address, select the IP address in the list, then click **Edit** to display properties, and then enter any changes. To remove an address from either list, select the address and click **Remove**.
Logging On to the Web Server

The web server is assigned a web address that can be used to open the WhatsUp Gold web page from any browser. This web address consists of the host name of the system on which WhatsUp Gold is installed, and the web server port number. The default port number is 80.

To log on to the web server:

1. Open any browser on your network and enter your WhatsUp Gold web address in the Address (or URL:) box. For example, if your WhatsUp Gold system is named `monitor1.ipswitch.com`, and uses port 8081, then the web address will be: `http://monitor1.ipswitch.com:8081`

   **Note**
   
   You can save your WhatsUp Gold web address as a “favorite” or “bookmark” site in your browser.

   After connecting, the logon dialog box appears.

2. Enter the user ID and password for your WhatsUp Gold web account. You may not have to enter a password, depending on how your WhatsUp Gold administrator set up access to the web server.

   The main page (“Top View”) for the WhatsUp Gold web server appears. You can use the views and functions provided to your web user account.

If your attempt to connect to the web server is denied, make sure the following have been done:

- Your WhatsUp Gold administrator has set up access to the web server for you.

- In **Configure->Web Server->General**, verify the **Enable Web Server** option is selected.

- Your computer’s IP address is allowed access in the **IP Security** dialog box (**Configure->Web Server->IP Security**).
What's Up Gold Web Display

After logging on to the What's Up Gold web site, you can use the following web pages (depending on your permissions): Top View page, Map View pages, Device View pages, Summary View pages, and the Events Log. This section briefly describes the views available from a web browser. Refer to the What's Up Gold web monitor's help system for detailed information.

Top View. The Top View page is displayed after you log on. It lists each active network map by map title (the title is set in Map Properties). You can click a map title to display the map page for that network.

Map View. Click a map name in the Top View to display the Map View. There are two formats for displaying maps in a web browser: Graphical maps, which use the same icons and colors as maps on the console; or a Text listing of devices in a map. To view the Graphical maps, select Enable Graphical Maps in the General dialog box.

Any services being monitored on a device are shown. The Map View will show any alerts that occur for devices in the map and will play an audible alarm (if your computer has a sound card). You can click Acknowledge to acknowledge the alert and turn off an alarm.
Text Listing view of a map. In this example, **Enable Graphical Maps** was NOT selected from **Configure->Web Server->General**.

Graphical maps view of a map. In this example, **Enable Graphical Maps** WAS selected from **Configure->Web Server->General**.
Device View. Click any device in the list to show its Device View. The Device View lists the host name, IP address, and polling statistics for the device. The polling statistics are the same as those displayed in the Statistics Window in the WhatsUp Gold application.

Summary View. The Summary View lists all devices in the selected network map and shows the polling statistics for each device.
Log View. You can click the Log View button to view the Event Log page. The Event Log page shows all events that have been logged for the devices in a network map.

WhatsUp Gold Web Functions

This section briefly describes the WhatsUp Gold functions available from a web browser. Refer to the WhatsUp Gold web monitor’s help system for detailed information.

The functions available to each user are determined by the permissions granted to the user account. For information on setting up web accounts, see “Setting Up User Accounts for the Web Server” on page 137.


Configure maps. Change settings for a selected map, such as map title, poll timer, and timeout.

Configure devices. Change the settings for a device, such as the display name, host name, IP address, polling frequency, polling schedule, and up and down dependencies.
Configure reports. Configure the recurring network status report. This report provides a snapshot of your network’s status (including Up and Down devices and down services) and can be sent via e-mail, pager, or beeper notification.

Configure users. Add, remove, and change WhatsUp Gold web user accounts.

Acknowledge alerts. Acknowledge a reported change (alert) and stop any further alerts for the change.

Access tools. Use the Ping, Trace, Lookup, and Scan tools. These tools operate from the system on which the WhatsUp Gold application is installed. For example, when you do a “trace” from the web interface, you are tracing the route from the WhatsUp Gold system to a remote system.
Chapter 8: Monitoring SNMP Devices

The Simple Network Management Protocol (SNMP) is an Internet standard that allows management data on different network devices to be read and monitored by an application. You can use WhatsUp Gold to view and monitor SNMP objects on any device that implements an SNMP agent.

This chapter describes how WhatsUp Gold implements SNMP, how to view and monitor SNMP values for a networked device, and how WhatsUp Gold can receive unsolicited messages (known as traps) from an SNMP device.

SNMP Implementation in WhatsUp Gold

This section provides an overview of the SNMP monitoring functions available in WhatsUp Gold. It assumes you are familiar with the SNMP standard and Management Information Base (MIB) for SNMP objects. For background information on SNMP and the MIB, see “SNMP Overview” on page 150.

WhatsUp Gold provides limited monitoring of devices that support SNMP. WhatsUp Gold supports the current Internet standards: SNMP Version 1 and MIB II. You can make custom extensions to MIB II to add vendor-provided SNMP objects. For more information, see “Setting Up the MIB Identifiers” on page 154.

Note

WhatsUp Gold does not let you change the value of an SNMP object on a device and does not provide SNMP manager functions.

Use WhatsUp Gold to do the following types of SNMP monitoring:

- View SNMP information on a device.

  You can use the SNMP tool (Tools->Net Tools->SNMP tab) to view information for a device.

- Graph selected SNMP values.
You can graph the SNMP values by using the SNMP Graphing Utility (Start->Programs->WhatsUp Gold->SNMP Graph Utility or from Tools menu, select WhatsUp Gold SNMP Graph Utility).

- Receive traps from SNMP devices.

A trap is sent when the status of a device changes. Traps are unsolicited messages, such as a router indicating one of its interfaces went down or a printer indicating it is out of paper.

WhatsUp Gold records traps on the Quick Status->Log of a device (found by right-clicking the device) and in the Event Log (provided Enable Logging is selected on Alerts in device properties). You can also set WhatsUp Gold to send a notification (via Beeper, Group, Pager, SMTPMail, Sound, WinPopup, or Voice) when a trap is received.

When a trap is recorded for a device, that device’s display name will be highlighted on the network map (as happens with any change in status). You can then check the Log dialog box in the device properties for the trap information.

- Monitor whether SNMP is running on a device.

You can select SNMP on the device properties Services and monitor it just as you can monitor any service. Again, this only checks to see if SNMP is running on the device; no SNMP management is involved.

The following sections describe how to use each of these capabilities.

**SNMP Overview**

The Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a networked device (a host, gateway, server, etc.). A monitoring or management application on the remote user’s system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device can provide information about the device’s network configuration and operations, such as the device’s network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a
standard format defined in the Management Information Base (MIB). The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol, together with the MIB, provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. For a detailed description of SNMP, see Request for Comments (RFC) 1157. For a description of the MIB, see RFC 1213.

**Note**

**Management Information Base (MIB)**
The MIB contains the essential objects that make up the “management information” for the device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

This section provides a brief description of the MIB. For a detailed description of the MIB, see RFC 1213:

The MIB is defined as an “object tree” divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:
• system — contains general information about the device, for example: sysDescr (description), sysContact (person responsible), and sysName (device name).

• interfaces — contains information about network interfaces, such as Ethernet adapters, or point-to-point links; for example: ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).

• ip — contains information about the processing of IP packets, such as routing table information: ipRouteDest (the destination), and ipRouteNextHop (the next hop of the route entry).

• Other groups provide information about the operation of a specific protocol, for example, tcp, udp, icmp, snmp, and egp.

• The enterprises group contains vendor specific objects that are extensions to the MIB.

The MIB provides an extensible design to which both public and private objects can be added.

Each object in the MIB has a numeric object identifier and a text name. For example, the system group contains an object named sysDescr, which provides a description of the device. The sysDescr object has the following object identifier:

```
iso org dod internet mgmt mib system sysDescr
1 3 6 1 2 1 1 1
```

This object identifier would be 1.3.6.1.2.1.1.1 to which is appended an instance sub-identifier of 0. That is, 1.3.6.1.2.1.1.1.0 identifies the one and only instance of sysDescr.

You will find all of the MIB-II objects (for TCP/IP networks) under the MIB node of tree (so all these objects will have an identifier that starts with 1.3.6.1.2.1).
Security

Limited security is provided for access to a device’s data by use of a community profile. The network administrator can assign a community name within the SNMP agent, or manager, on a device. The network management application can access data on the device only if it knows the community name.

Most SNMP agent software (on the device) also let you specify the IP addresses from which the agent will accept requests.

SNMP Agent or Manager

SNMP agent or manager software must be installed and enabled on any devices from which you want to receive SNMP information. Windows NT, Windows 2000, 98, and 95 provide an SNMP agent. Network systems manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

SNMP Operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

- Get — gets a specified SNMP object for a device
- Get next — gets the next object in a table or list
- Set — sets the value of an SNMP object on a device
- Trap — sends a message about an event (that occurs on the device) to the management application

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using UDP. Trap messages, which are unsolicited messages from a device, are sent to port 162.

If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.
SNMP Traps

The SNMP standard provides a limited number of unsolicited messages (called traps) that are sent from a device to an SNMP application. These messages can be sent by the SNMP agent on the device to notify an SNMP application of a change in status.

There are six standard traps which you can receive from any SNMP agent and there can also be enterprise specific traps for a device, which are defined by the device vendor.

Traps are numbered as follows:

<table>
<thead>
<tr>
<th>Trap #</th>
<th>Trap type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Cold start</td>
<td>The device is rebooting itself and may change its configuration or the SNMP agent’s configuration.</td>
</tr>
<tr>
<td>1</td>
<td>Warm start</td>
<td>The device is rebooting itself but neither the device’s nor the SNMP agent’s configuration will change.</td>
</tr>
<tr>
<td>2</td>
<td>Link down</td>
<td>One of the communication links for the device is down.</td>
</tr>
<tr>
<td>3</td>
<td>Link up</td>
<td>One of the communication links for the device is back up.</td>
</tr>
<tr>
<td>4</td>
<td>Authorization failure</td>
<td>The device has received a protocol message that is not properly authenticated.</td>
</tr>
<tr>
<td>5</td>
<td>EGP neighbor loss</td>
<td>An EGP neighbor for which the device is an EGP peer is down and the peer relationship no longer exists.</td>
</tr>
<tr>
<td>6</td>
<td>Enterprise specific traps</td>
<td>The SNMP specification lets vendors define enterprise specific traps, for example a trap that occurs on a particular vendor’s router. Enterprise specific traps should be added to the MIB on the device and on the management application.</td>
</tr>
</tbody>
</table>

Setting Up the MIB Identifiers

WhatsUp Gold uses two reference files (mib.txt and traps.txt) to refer to MIB identifiers. The reference files are used by WhatsUp Gold to display the MIB object tree when you browse for an object name/identifier using the SNMP tool.
As shipped with WhatsUp Gold, these reference files contain the SNMP objects defined in the MIB-II standard, including the six standard SNMP traps.

If your network includes devices from a vendor who also provides RFC-compliant MIB files, you can update these reference files to include the MIB and trap information from the vendor’s files; to do this, you run the MIB Extractor.

The WhatsUp Gold “MIB Extractor” (a command line program named mibextra.exe) updates the MIB and trap information that WhatsUp Gold references when it converts SNMP object and trap identifiers into object and trap names, and vice versa.

To run the MIB extractor:

1. Collect your vendor-provided MIB files into a single directory
2. At the command prompt, enter:
   
   mibextra directoryname\filename
   
   where filename is the name of the vendor-provided file.

The MIB Extractor reads the current contents of mib.txt and traps.txt, processes the vendor-provided MIB files, and rewrites mib.txt and traps.txt.

**Note**

If the MIB Extractor returns a “failed to open file” error, the MIB file you are using has dependencies. These "dependency" files are listed in the Import section of the vendor’s mib file. You should check all of the MIB files for dependencies.
Viewing SNMP Objects

The SNMP tool lets you view information on a remote device that has an SNMP agent. To view SNMP information:

1. From the **Tools** menu, select **Net Tools**, and click the **SNMP** tab to display the SNMP options.

2. In the **Address** box, enter the host name or IP address of the device for which you want to view SNMP objects, or select one from the list box.

3. If necessary, change the text in the **Community** box. The default string is “public.”

SNMP (Version 1) as a protocol does not support security. Security is implemented within the SNMP manager itself (on the device) by specifying the IP addresses from which it will accept requests. However, simple security can be implemented by use of the community string.

The default string (public) will work for most SNMP hosts unless the administrator has specifically removed public and replaced it with a string of his/her own. If you know a device is manageable via SNMP and “public” doesn’t work, you will have to talk to the owner of that device to get a community name that will work.
4 In the **What** box, type an SNMP object name or identifier to retrieve, or click the button next to the **What** box to display the MIB tree view of the SNMP objects.

![SNMP Object Selecte](image)

Each SNMP object has a name and numeric identifier. For example, in the “system” group, the network object named `SysDescr` with object identifier 1.3.6.1.2.1.1.1 contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the `ifPhysAddress` object, which has object identifier 1.3.6.1.2.1.2.1.6. In this case, you need to specify an instance number at the end of the object identifier (such as 1.3.6.1.2.1.2.1.6.1). If you do not specify an instance number, it defaults to zero. For more information on SNMP objects, see the “SNMP Backgrounder” section of this chapter.

---

**Note**

Entering `*sysInfo` in the **What** box returns most of the “system” identification objects.
Select one of the radio buttons:

**Get.** If you know the object name or identifier, you can enter it in the What box and use the **Get** option. For example, on a Windows NT system, a **Get** request for ifPhysAddress.2 returns the network adapter address. If it is a wrong name or number, you will not get any information back. If there is more than one instance of the object, you need to enter the specific instance.

**Get Next.** Use **Get Next** to get the next object instance from a table or list within the SNMP agent on the device. You can determine the values to use in the What box by what is returned using **Get Next**. You should use this option with most of the items that are in the MIB.

**Get All Subitems.** This option returns any subitems of the named item.

**Monitor.** Starts the SNMP Graphing Utility and graphs the network object specified in the What box. For more information on graphing, see “Graphing SNMP Values” on page 159.

(Optional) Change the **Delay** setting from the default of 1000 milliseconds. This value tells the SNMP tool how long to wait for a response to an SNMP request before reporting a timeout.

Click **Start** to retrieve the SNMP information.

Any information found for the object is shown in the results window.
Graphing SNMP Values

Some of the SNMP objects are best monitored by displaying their changing values in a graph. WhatsUp Gold’s SNMP Graphing Utility lets you select one or more SNMP objects and show a real-time graph of their values. You can also save a particular graph and later open the graph to resume graphing the SNMP objects.

The main window of the SNMP Graphing Utility shows a line graph for each SNMP object added to the graph.

Up to 20 SNMP objects can be active on the graph. You can set the color and line width to distinguish each graphed object.

By default, the SNMP Graphing Utility graphs the change between each reported value of the SNMP object. You can set the utility to graph only the reported values for an object. For more information, see “Adding, Editing, and Deleting SNMP Objects” on page 160.
starting the snmp graphing utility

to start the snmp graphing utility, do one of the following:

- from the tools menu, select snmp graph utility; or from the start menu, select programs->whatsup gold->whatsup gold snmp graph utility.

  the utility starts the default graph file (graph.wgg) that shows the time elapsed between snmp values reported, which is determined by the interval specified in graph->properties.

- from the snmp tool (tools->net tools->snmp tab), enter an snmp object identifier in the what box, select monitor, and then click start. the whatsup gold graphing utility appears and begins real-time graphing of the selected snmp object.

adding, editing, and deleting snmp objects

to add an snmp object to the graph:

1. from the edit menu, select add item->snmp item. the graph item properties appear:

   2. in the host box, enter the host name or ip address of the device for which you want to graph snmp objects, or select one from the list box.
3 If necessary, change the string in the Community Name box. The default string is “public.” The default (public) will work for most SNMP hosts unless the administrator has specifically removed “public” and replaced it with a string of their own. If you know a device is manageable via SNMP and public doesn’t work, you will have to talk to the owner of that device to get a community name that will work.

4 Enter the Item and Instance numbers to specify the SNMP object that you want to graph. (Use the Browse button to the right of the Item box to view the MIB tree and select an object. When you select an object in the MIB tree, its object identifier is entered in the Item box.)

For background information on item and instance numbers, see “SNMP Overview” on page 150. To customize the MIB tree to include vendor-provided objects that are specific to your enterprise, see “Setting Up the MIB Identifiers” on page 154.

5 Set the item graphing options:

Absolute values. When selected, graphs the reported values of an SNMP object rather than graphing the change between the last reported value and the current value (default method). You probably want to turn off Absolute values when graphing a counter, such as ifOutOctets; otherwise, the graphed values may be difficult to read.

AutoScale. When selected, the graph scale for the SNMP object is determined by the graphing utility. This is a relative scale that is calculated to make the graph fit into the vertical scale. If you turn off this option, the Scale option becomes active and you can enter a value to scale the graph.

Bytes to bits. When selected, multiplies the value reported for the SNMP object by 8 to approximate the count in bits. This option can be used with SNMP objects that are counters, for example if you want to know the baud rate while monitoring a T1 router port, you want (ifOutOctets * 8) to give you a value close to the real baud rate.
**Reset values.** When selected, clears the values for the selected SNMP object when you exit the dialog box. You can clear the values for all SNMP objects on the graph by selecting **Clear** from the **Edit** menu.

**Line width.** Sets the width of the line that represents the selected SNMP object.

**Color.** Sets the color of the line that represents the selected SNMP object.

**Scale.** When **AutoScale** is turned off, you can enter a fixed value in this text box to determine the scale of the graph. You may want to try different values in this box until you find a scale that is useful.

**Rate per second.** When selected, calculates the average change per second in the values reported for the SNMP object, and then graphs the result. To calculate this average, it takes the difference between the latest reported value and the previously reported value, then divides by the number of seconds between reported values. This option is useful when the graph **Interval** (in Graph Options) is different than one second. You cannot use this option with the **Absolute values** option.

Click **OK** to add the SNMP object to the graph.
**Viewing Item Values**

You can view the raw data used to generate the graph for an SNMP item. Select the graph item in the Legend, then from the Edit menu, select **View Item Values**.

The “View Item Values” window shows the following data for the SNMP object:

**Title bar.** Shows the IP address of the selected host and the object identifier for the SNMP object.

**Time.** Time the value was reported.

**Value.** The absolute value reported by the SNMP object.

**Diff.** This is the difference between the reported value and the previously reported value. (Note that this value may not make sense if the graph is at a “wrap” point.)
Reported. This is the actual value used in the graph. This value depends on the setting in the graph item’s properties, which can be set in one of the following dialog boxes: Graph Item Properties, Graph Accumulator Properties, Graph Timer Properties. If the item is set to report Absolute value, this value will be equal to the absolute value. If set to report Bytes to bits, this value will be the absolute value multiplied by 8. If set to report Rate per second, this value will be the difference between the last two reported absolute values divided by the time difference (Time Diff). If both Bytes to bits and Rate per second are selected, the reported value will be equal to the difference between the last two reported absolute values multiplied by 8, then divided by the time difference (Time Diff).

Time Diff. This is the difference (in milliseconds) between the time the last value was reported and the time the previous value was reported.

Click Refresh to update the displayed values.

Editing Item Properties

To edit a graph item’s properties:

1 To select the item to edit, do one of the following:
   • In the graph legend, double click the item you want to modify.
   • In the graph legend, click the item you want to modify, and then from the Edit menu, select Item Properties.
   • In the graph legend, right-click the item you want to modify, and from the right-mouse menu, select Properties.
Monitoring SNMP Devices

The following dialog box appears.

![Graph Item Properties dialog box](image)

2  Make any changes to the properties and click **OK** to save them and exit the dialog box.

**Deleting Items from the Graph**

You can delete an item from the graph at any time. In the graph legend, do one of the following:

1  Click the item you want to delete, and then from the **Edit** menu, select **Delete Item**.

2  Right-click the item you want to delete and then from the right mouse menu, select **Delete**.

**Saving and Opening Graph Files**

You can save a graph to a file and it will save the selected graph items and options. Data values are not saved. You can later reopen the graph file and resume real-time graphing of the saved SNMP items. WhatsUp Gold SNMP graph files use the extension `.wgg`.

To save a graph:

1  From the **File** menu, select **Save Graph**. The “Save As” dialog box appears.

2  In the **File** name box, enter a file name with a `.wgg` extension.

3  Click **Save** to save the graph objects.
To open a saved graph:

1. From the **File** menu, select **Open Graph**. The “Open” dialog box appears.
2. Select a graph file name (with a .wgg extension) and click **Open**.

**Editing Graph Properties**

Use the “Graph Options” dialog box to set the layout of the graph window, the interval (or frequency) for recording values for the SNMP objects, and whether you want to record the data to a file.

To view the properties: from the **Graph** menu, select **Properties**.

**Legend.** When selected, the Legend appears at the bottom of the graph window. The Legend displays each graphed SNMP object and its associated device, as well as any accumulator items.

**Interval (seconds).** Sets the time interval at which the graph records values.

**Vertical** (y-axis). When **Grid** is selected, displays lines across the graph to help you read the vertical graph. When **Labels** is selected, values are displayed next to the y-axis. The **Maximum** determines the highest value on the y-axis scale, as well as the internal values. This value cannot exceed 1500.

**Horizontal** (x-axis). When **Grid** is selected, displays lines across the graph to help you read the x-axis values. When **Labels** is selected, values are displayed next to the x-axis. The **Maximum** determines the highest value on the x-axis, as well as the internal values. This value cannot exceed 1500.
**Save Window Location.** When selected, saves the position of the Graph Window so that it always opens in the same location on your screen.

**Record data to.** If you want to save graph data, select this box and enter a file name. Whenever the graph is running, the SNMP values will be appended to this file. The file is saved in the WhatsUp Gold directory. The file format is tab-delimited and can be imported to a spreadsheet application.

File Format:

Date [tab] time [tab] first item value [tab] second item value [tab] ...

For example, a graph with three items would show the date and time plus the three values recorded at that time. The heading shows the IP address and SNMP object identifier for each graph item.

```
[156.21.50.12]:1.3.6.1.2.1.2.2.1.10.3
[156.21.50.12]:1.3.6.1.2.1.2.2.1.10.4
[156.21.50.12]:1.3.6.1.2.1.2.2.1.16.3
```

01/03/2001 11:07:34 103782671006689
01/03/2001 11:07:35 169587431031456
01/03/2001 11:07:36 20678156873944

---

**Receiving SNMP Traps**

WhatsUp Gold has an internal SNMP trap handler, which when enabled, listens for and accepts SNMP traps that are addressed to it. A trap is sent when the status of a device changes. Traps are unsolicited messages, such as a router indicating one of its interfaces went down or a printer indicating it is out of paper.

When a trap arrives from a device, WhatsUp Gold highlights the device’s display name on the network map to show a status change and records the trap information in the device’s Log dialog box (found by right-clicking a device, selecting **Quick Status»Log**), and in the Event Log.

You can also set up WhatsUp Gold to send a notification message (via Beeper, Group, Pager, SMTPMail, Sound, WinPopup, or Voice) when a trap is received for a device.
To receive traps in WhatsUp Gold, you need to do the following:

1. On each physical device that will be monitored, set the SNMP agent to send traps to WhatsUp Gold. This cannot be done from WhatsUp Gold.

2. If you have vendor-provided devices, run the MIB Extractor as described in “Setting Up the MIB Identifiers” on page 154.

   Enable the SNMP Trap Handler. (Select Configure->Program Options->SNMP Traps, select Enable SNMP Trap Handler, and then click OK.

3. Set up any notifications for traps as described in the following section.

**Setting Up Notifications for Traps**

You can set up WhatsUp Gold to send a notification when an SNMP trap is received for a device. You can specify that the notification is sent when any trap message is received or when a specified trap number(s) is received. For background information about SNMP traps and trap numbers, see “SNMP Traps” on page 154.

To set up a notification for a trap message:

1. Double-click the device and click **Alerts**.
Note
To do this for a subnet icon or container icon, right-click the icon, select **Properties**, and click **Alerts**.

2 Select **Enable Alerts** and **Enable Logging**.

3 In the Alerts section, click **Add**.

The “Add Notifications” dialog box appears.

4 From the list box, select the notification you want to send when this device receives a trap message.

You can create new notifications and make them available in the list box. See the “Defining Notifications” section in Chapter 5 for the step-by-step procedure.

5 Select the **On SNMP Trap** option.

When this option is enabled, and the edit box to the right of it is empty, the specified notification will be sent when *any* trap is received for the device. If the edit box contains a trap number or numbers, notification is sent only if a trap with the specified number is received. Separate multiple entries in the text box with a comma.

**Example:** To limit notifications to certain enterprise-specific SNMP traps, enter both the major and minor trap information separated by a period.

The trap syntax is: displayname,SNMP_object_id,major_trap,minor_trap (where
enterprise names appear for SNMP_object_id).
For example, your traps.txt file might contain the following two traps.

- badVoltage,apc,6,49
- batteryOverTemperature,apc,6,53

To be notified upon receipt of one of the traps, enter 6.49 or enter 6.53 in the 'On SNMP Trap' field.

To be notified upon receipt of both traps, enter 6.49,6.53 in the 'On SNMP Trap' field.

Major and minor trap numbers are separated by periods. Multiple trap entries are separated by commas.

You can enter a number for one of the six standard traps, or you can enter a number for a vendor-provided trap. If you are unsure of a trap number, you can view the Event Log (after enabling traps) to see what number is associated with a particular trap.

Note that the notification of the SNMP trap is sent as soon as the trap arrives: the Trigger value is ignored. The trap text can be included in mail notifications if you use the %N variable. For more information, see “Notification Message Variables” on page 66.

---

**Note**

A notification will also be sent if the device misses the number of polls specified in the Trigger box. If you want to be notified only of an SNMP trap, you can set the Trigger to 9999.

---

6  Set the **Time Period** in which you want the notification to be active.

7  Click **OK** to save your changes. The notification is added to the device’s list of notifications.

8  In **Alerts**, click **OK** to save changes and exit the dialog box.
**Viewing Trap Log Entries**

SNMP traps are logged regardless of whether or not you have enabled log activity for the device.

To view trap information for a device, right-click the device, select **Quick Status** and click **Log**.

To view trap information for all devices, from the **Logs** menu, select **SNMP Trap Log**.

---

**Monitoring SNMP Service**

To monitor whether SNMP is running on a device:

1. Double click the device to display its properties.

   **Note**

   To do this for a subnet icon or container icon, right-click the icon, select Properties, and then click **Services**.

2. Click **Services** to display services properties.

3. In the **Services to Monitor** box, select the **SNMP** service.

4. Click **OK** to apply the changes and exit the dialog box.

**NOTE:** If SNMP service is being monitored on a device, a small triangle is displayed in the upper-corner of the device’s icon in the map. If the device is an SNMP manageable device, then a small star appears in the upper-corner of the device’s icon in the map.
Chapter 9: Using Network Tools

WhatsUp Gold includes a versatile set of tools that let you search for and display information about organizations, networks, computers, or people on a network.

From the Tools menu, when you select Net Tools you see the following tabbed dialog box:

Each tab contains the parameters and results area for one tool. The tools include:

- **Info** — Display a summary of device information.
- **Time** — Synchronize your computer’s clock with a remote time server.
- **HTML** — Query a web address.
- **Ping** — Verify connectivity to a host.
- **TraceRoute** — Trace and view the route to an Internet host.
- **Lookup** — Query Internet domain name servers for information about hosts and name servers.
- **Finger** — Display information about users on a host.
• Whois — Display information from the network information center about Internet domain ownership and Internet groups.
• LDAP — Search directories for names and information.
• Quote — View quotations from a quote server.
• Scan — Scan a range of IP addresses to create a network map. For information on using this tool, see “Chapter 2: Creating Network Maps” on page 13.
• SNMP — View and graph Simple Network Management Protocol values for a device. For information on using this tool, see “Chapter 8: Monitoring SNMP Devices” on page 149.
• WinNet — View Windows Network domains, hosts, and workstations.
• Throughput — Test data throughput on the connection between your computer and a remote computer.
• System Info — View information about your local system.

Using Format, Copy, and Print Functions

You can use the standard Windows cut, copy, and paste functions in all the tools and you can cut, copy, and paste between the tools as well as between a tool and any Windows application.

In general, to cut, copy, or paste data in a text box or in a display window, you can click the right mouse button to display the pop-up menu.

However, the right mouse menu is not available when you are using the Report View of the Ping, TraceRoute, and Throughput tools; use the Edit menu instead. Furthermore, when using the Info tool, you can select and copy text only when displaying results in the List View.

Printing Results

You can print the results displayed by any of the tools. Within a tool’s tab, display the results of a query, and then from the File menu, select Print to view the standard Windows print setup dialog box.
Displaying Device Information (Info Tool)

The Info tool displays a summary of information about a network host or device, including the official host name, IP address, and contact information (from the Whois database). An Info request on a host name also polls (pings) the host to verify connectivity.

The Info tool provides a quick way to get host information – it runs Lookup and Whois queries on the specified host and also pings the host to check its availability.

To send an Info query:

1. From the Tools menu, select Net Tools and click the Info tab to display the Info options.
2. In the Host name or IP Address box, enter the name or address of a host you want to query. This must be a fully qualified host name or address (for example: whitehouse.gov)
3. Click the Start button.

The results of the query appear in the window.

During the query, the Start button toggles to Stop. You can click Stop at any time to stop the query. Click Clear to erase the results from the display window.
Checking a Web Address (HTML Tool)

The HTML tool’s primary purpose is to help developers debug their web sites. The HTML tool sends a “get” or “head” request to a specified web address (URL) and returns full header information (including cookies) and also returns the page data (raw or formatted HTML code).

To query a web address:

1. From the Tools menu, select Net Tools and click the HTML tab to display the HTML options.

2. In the URL (Uniform Resource Locator) box, enter the web address of the web page you want to query.

   This must be a specific web site file (for example: http://hostname/page/). A slash (/) is required at the end of the URL.

3. Select the format for displaying the page data: Select Raw to display page data with embedded HTML code. Select Formatted to display the page data with carriage returns inserted. Select Interpreted to display the page as viewed in a browser. Select Header only if you want to display the HTML header for the page, without downloading the full contents of the page.

4. Click the Start button.

The results of the query appear in the window.
During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

### Synchronizing Time (Time Tool)

The Time tool lets you synchronize your local system’s clock with the clock of a remote time server. Remote time servers provide a constantly updated time of day reading (in hours, minutes, and seconds) and the date (year, month, day). The Time tool provides predefined entries for some publicly available time servers. You can also query your own or other time servers.

**Note**
The Time tool uses the Time protocol specified in RFC 868.

Using the Time tool, you can also:

- Synchronize your local clock on demand
- Interrogate multiple time of day servers simultaneously and display the difference (in seconds) between the remote time server and the local system time.
- Adjust the displayed time of a remote time server by setting an offset (plus or minus hours) from GMT.
- Sort the display (for multiple time servers) by column (Server Name, Time, Difference, Offset, and Error Code).

To synchronize your local system’s clock with a remote time server:

1. From the **Tools** menu, select **Net Tools** and click the **Time** tab to display Time options.

2. In the **Time Server** box, type the host name or IP Address (for example, xfiles-jr.esa.lanl.gov, navobs1.wustl.edu, wwwvb.isi.edu) of the remote time server you want to query. The list box shows the previous host names or IP addresses you have queried.

3. Select the **Synch Clock to Remote Time** option (make sure it is checked). Your local system’s date and clock time is always displayed above the results area.
4 Optionally, use the **Offset** box to adjust the displayed time of a remote time server by an offset (plus or minus hours) from GMT.

5 Click the **Start** button.

A connection is established with the remote time server and the server name and current time are reported in the display window. The reported time is constantly updated until you do one of the following:

- Click **Clear** to clear the display.
- Select the time server in the display, and then select **Remove** from the right-mouse menu.

The display window also shows the time difference between your local system’s clock and the time server’s clock, any time offset you specified, and any error codes reported. (If Time reports an error code, try another time server from the list.)

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

To sort values in a column in ascending order, click the column heading. To reverse the sort order, click again.
To interrogate multiple time servers:

One at a time, enter or select the time server’s host name or IP address in the Time Server box and then click Start. Each time server you select is displayed on a separate line.

To update the time reported by the server now:

Right-click the time server in the Server Name column to display the pop-up menu, and then select Update Time from Server.

To synchronize the local clock with the time server now:

Right-click the time server in the Server Name column to display the pop-up menu, and then select Sync Clock To Remote Time.

To suspend polls to a time server:

Right-click the time server in the Server Name column to display the pop-up menu, and then select Stop Monitoring This Item. To restart monitoring, right-click on the server and select Start Monitoring This Item.

To suspend polls to all time servers:

Right-click any time server in the Server Name column to display the pop-up menu, and then select Stop Monitoring All Items. To restart monitoring, right-click on any server and select Start Monitoring All Items.

To remove a time server from the list of servers:

Right-click the time server in the Server Name column to display the pop-up menu, and then select Remove.

To change the offset (to account for time zone differences):

1. Click the time server in the Server Name column or select a server from the Time Server list box.

2. In the Offset list box, select the desired offset.

3. Click Start.
Verifying Connectivity (Ping Tool)

The Ping tool is a network diagnostic tool used to verify connectivity to a particular system on your network. Ping sends an ICMP “echo request” in the form of a data packet to a remote host and displays the results for each “echo reply”. This exchange is referred to as “pinging.” The Ping command also displays the time for a response to arrive in milliseconds (this will vary depending on network load) and debugging information about the network interface. You can have multiple instances of the Ping tool active simultaneously.

To ping a host:

1. From the Tools menu, select Net Tools and click the Ping tab to display ping options.

2. In the Host name or IP Address box, type a host name or IP Address (for example, internic.net).

3. Select the protocol to use for pinging depending on the type of host selected. Use ICMP for TCP/IP hosts, IPX for Novell NetWare hosts, or NetBEUI for Windows network hosts.

   **Note**

   To ping an IPX device, Microsoft’s NWLink IPX/SPX Compatible Transport must be installed and running on the WhatsUp Gold system. For more information, see “System Requirements” on page 6.

4. Set any of the options you want to use:

   - **Count.** The number of data packets sent by the ping command.
   - **Delay (sec.).** Number of seconds to wait between sending a ping.
   - **Size.** The length in bytes of each packet sent by the ping command.
   - **Timeout (ms).** The ping will fail if the host does not respond after this number of milliseconds.

5. Click the Start button.
The Ping tool sends an echo request and waits for the echo reply. If the ping was successful, summary lines are displayed in the Ping tab, indicating the result of the ping.

If the reply is not received within the timeout value, the ping fails. This means there has been a failure at one of several points from your PC to the remote host. The host may not be functioning and therefore is unable to respond, a network or gateway in the path from the user may not be working, or the host may not implement the service you are requesting.

During the ping, the Start button toggles to Stop. You can click Stop at any time to stop the ping. Click Clear to erase the results from the display window.

**Tracing a Route (TraceRoute Tool)**

The Traceroute tool lets you trace and view the actual route an IP packet follows from the local host to another host on the Internet. Response times are displayed in milliseconds and will vary depending on network load. TraceRoute is useful for finding potential trouble spots on large and complex networks that are connected together by routers.

The results of a traceroute can be mapped to a network map.
To initiate a traceroute search, do the following:

1. From the **Tools** menu, select **Net Tools** and click the **TraceRoute** tab to display the traceroute options.

2. In the **Host Name or IP Address** text box, enter a host name or IP address for the remote host — this is the host to which you want to trace the route.

   The list box shows the previous host names or IP addresses for which you’ve done a traceroute.

3. Set any of the options you want to use.

   **Maximum Hopcount.** The maximum number of hops to trace before ending the traceroute. When an IP packet passes from one host to another, it is referred to as one hop.

   **Map Results.** When this option is enabled, when you launch a trace to a host, WhatsUp Gold draws a map of the route, displaying an icon for each router and showing the connections from router to router until it reaches the host.

   **Resolve Addresses.** When enabled, the host names of each router along the route will be displayed along with the IP addresses. When disabled, only the IP addresses are shown. Showing the host names will add time to the traceroute as it requires that the IP addresses be resolved.

   **Set Dependencies.** This option is available when **Map Results** is selected. When enabled, it will set each router found by the traceroute as an “up” dependency on the previous router in the route. This means that when polling, if a router is down, WhatsUp Gold will not poll routers further along the route to a host.

   **Timeout.** The TraceRoute will fail if the device does not respond after this number of milliseconds.

4. Click the **Start** button.

   The results of the TraceRoute search are displayed in the results area.
During the trace, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the trace. Click **Clear** to erase the results from the display window.

If the **Map Results** option is enabled, WhatsUp Gold draws a map of the route. It adds icons for any devices (such as routers) that are not already in the map. The following example shows the map of the route from Sleepy (the local host) through each router along the path to the Internet’s host.
Finding Host and Name Server (Lookup Tool)

The Lookup tool lets you query Internet domain name servers for information about hosts and name servers. You can use Lookup to:

- Find the IP address from a name or a name from an IP address
- List just the name and Internet address of a host or domain
- Query the name server for information about various hosts and domains
- List hosts in a domain

To initiate a Lookup query:

1. From the Tools menu, select Net Tools and click the Lookup tab to display lookup options.
2. In the Name or IP Address text box, enter a host name or IP address of the device or domain name server you want to look up.
3. Set any of the options you want to use.

   **DNS Server:** Enter the IP address of the domain name server you want to query or select [stack] from the list box to use the network stack in your operating system.

   **Note**

   When you select the [stack] option, Lookup uses the Winsock stack lookup routines. If you specify a server, Lookup creates and interprets its own DNS packets and does not use the Winsock stack routines.
**Query Type.** Select a type from the list box. The query types are:

<table>
<thead>
<tr>
<th>Type</th>
<th>Returns the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The host’s Internet address</td>
</tr>
<tr>
<td>ALL</td>
<td>All information</td>
</tr>
<tr>
<td>CNAME</td>
<td>Alias names for the host</td>
</tr>
<tr>
<td>HINFO</td>
<td>The CPU type and operating system type of the host</td>
</tr>
<tr>
<td>MX</td>
<td>The host that acts as the mail exchanger</td>
</tr>
<tr>
<td>NS</td>
<td>The name server for the named zone</td>
</tr>
<tr>
<td>PTR</td>
<td>The host name, if the query is an Internet address; otherwise, a pointer to other data</td>
</tr>
<tr>
<td>SOA</td>
<td>The domain’s “start of authority” information, which indicates the name server and additional administrative information</td>
</tr>
<tr>
<td>ZONE</td>
<td>The zone listing for the domain, which defines the domains for which the name server is the primary name server and lists registered host in the domain</td>
</tr>
</tbody>
</table>

**Note**

If you use the network stack, you can only do name-to-address lookups (A) or address-to-name lookups (PTR). If you specify a DNS server, you can use all of the query types.

The **Verbose** option is useful only when you specify a DNS server. When enabled, you can see the information that comes back from the DNS server.
4 Click **Start**. The information returned by the lookup query appears in the results area.

![Net Tools Interface](image)

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

---

**Getting Information About Users (Finger Tool)**

The Finger tool lets you identify and display information about all users on a network host. This information can include a display of current users on the host (their user IDs and user names), and for each user — the home directory, log in time, idle times, office location, last time they received mail, and last time they read mail. The exact data returned by a Finger query depends on what the source (the Finger server) has chosen to provide.

A Finger request will also display any information contained in the file `.plan` or the file `.project` in the user’s home directory. These files are often used as a simple way to distribute information.

If the specified host does not have a Finger server, the Finger client displays the message: **Connection not made**

To initiate a Finger query, do the following:

1 From the **Tools** menu, select **Net Tools**, and click the **Finger** tab to display Finger options.
2 In the **Finger String** text box, enter a host name or IP address. The list box shows the previous host names or IP addresses for which you sent a Finger request.

3 Click the **Start** button. The Finger client contacts the host’s Finger server. The results of the query appear in the window.

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

### Getting Owner Information (Whois Tool)

The Whois tool, like Finger, is an Internet directory service. Whois provides information about who owns an Internet host or domain and who you can contact regarding that host or domain. A Whois request displays a contact name, mailing address, telephone number, and network mailbox for all users and organizations who are registered with the Network Information Center (NIC) database.

**Note**

The current host server for the Network Information Center (NIC) is `whois.networksolutions.com`. You can send a Whois query to this host to display information on using services that the NIC provides.

To initiate a Whois query, do the following:
1. From the **Tools** menu, select **Net Tools**, and click the **Whois** tab.
2. In the **Search String** text box, enter a search string. If you know the name or handle of an organization, enter it here.
3. In the **WAIS Host** text box, enter a host name or user name.
4. Click the **Start** button. The Whois client contacts that host’s Whois server. The results of the query appear in the window.

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

### Searching Directories (LDAP Tool)

Lightweight Directory Access Protocol (LDAP) is an Internet standard for accessing directory information stored on a server. It permits an LDAP-enabled client to search for and view information stored in an LDAP directory on another computer. LDAP is a subset of the x.500 directory access protocol.

The LDAP tool lets you view information on a remote computer that has an LDAP server. Most LDAP servers will let you view e-mail addresses and users’ full names, and many servers will provide information such as the user’s organization name, division or department name, and postal address. In addition, any LDAP server can contain its own customized set of attributes or data.
To view LDAP information:

1 From the Tools menu, select Net Tools, and click the LDAP tab to display the LDAP options.

2 Define a query for LDAP information.

   Use the three text entry boxes at the top of the LDAP tab to specify a query for LDAP information.

   In the first text box, enter the LDAP attribute that you want to display, or select an attribute from the list box. If you want to display all the entries for the selected attribute (for example, you want to display all mail addresses), you can ignore the other two text boxes.

   If you want to further narrow your search to display specific entries, you can use the second and third text boxes. In the second text box, you can select one of the following:

<table>
<thead>
<tr>
<th>contains</th>
<th>the text (in the third box) is part of the entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>is</td>
<td>the text is the exact name of the entry</td>
</tr>
<tr>
<td>is like</td>
<td>the text is a near match for the entry (not supported by all LDAP servers)</td>
</tr>
</tbody>
</table>

   Then, in the last text box, you can enter criteria (such as a name) to display only those entries that meet the search criteria. For example, to search an LDAP directory for information about a company named Acme, you could enter it as follows:

   | FullName | contains | Acme |

3 In the LDAP Host box, enter the name of the host that you want to query.

   This must be a fully qualified host name (for example, mail.acme.com). From the list box, you can select some of the more widely-used LDAP directories. Your previous LDAP entries are also shown in the list box.
4 Click the **Start** button.

Any LDAP information that meets the specified search criteria is displayed.

![LDAP search interface](image)

**Note**

If there are too many responses to your query, most LDAP servers will not return anything. You’ll need to further define your search criteria.

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

**Viewing Quotations (Quote Tool)**

The Quote client lets you view information on a remote host that supports a Quote server. Quote servers often display a “quote of the day.” For example, if you connect to the Ipswitch quote server, you may see a quote like the following:

“It was as true as taxes is. And nothing’s truer than them.”

Charles Dickens (1812-1870)
To view Quotes:

1. From the **Tools** menu, select **Net Tools**, and click the **Quote** tab to display the Quote options.
   
   This must be a fully qualified host name (for example: `quotes.ipswitch.com`).

2. In the **Quote server** box, enter the name of a host that contains the quote server.

3. Click the **Start** button.
   
   The results of the query appear in the window.
   
   During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

---

**Scanning Your Network (Scan Tool)**

The Scan tool lets you scan a range of IP addresses to create a map of the devices in your network. For more information, see “Chapter 2: Creating Network Maps” on page 13.

---

**Viewing and Graphing SNMP Values (SNMP Tool)**

The SNMP tool lets you view and graph Simple Network Management Protocol values for a device. The device must be SNMP enabled. For information on using this tool, see “Chapter 8: Monitoring SNMP Devices” on page 149.

---

**Displaying Network Information (WinNet Tool)**

The WinNet tool scans your local network and displays the names of Windows network resources (domains, hosts, or shared resources). Note that resources on the Windows network use NetBEUI (Windows NetBIOS) names which may or may not correspond to Internet host or domain names. You can use the list box to select the items for which you want to scan. In addition, you can enter the NetBEUI name of a Windows resource on your network and view information about that resource.

1. From the **Tools** menu, select **Net Tools**, and click the **WinNet** tab.
In the **Network Items** list box, select the type of network items that you want to display from the list box. You can select from the following item types:

- **networks** — show all networks (groups of domains)
- **domains** — show all domains (groups of servers)
- **servers** — show all devices running the Server service
- **shares** — show all shared devices, such as printers
- **all** — show all the above types of items

Click the **Start** button.

WhatsUp Gold scans your local network and displays the name and address of the specified items.

During the scan, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the scan. Click **Clear** to erase the results from the display window.

---

**Testing Data Speed (Throughput Tool)**

Throughput is a diagnostic tool that lets you test the data speed on a connection with a remote host. It sends a specified number of IP packets, in a range of packet sizes, to a specified remote computer and calculates the average data speed over the communications link.

To test throughput on a connection:

1. From the **Tools** menu, select **Net Tools** and click the **Throughput** tab.
2. In the **Hostname** or **IP Address** box, type a host name or IP Address (for example, internic.net).
3. Set any of the options you want to use:
   - **Packet Count**. The number of data packets sent.
   - **Timeout (ms)**. The time, in milliseconds, that the tool will wait for a response.
   - **Packet Size**. The maximum length in bytes of the largest packet sent. To accurately determine throughput, use the largest packet size that works consistently without timing out.
   - **Delay (ms)**. Number of milliseconds to wait between packets.
**TCP.** Normally, ICMP packets are sent, but if this is selected, TCP checks are sent through the echo port (port 7), which must be running on the remote system. Throughput is more accurate if this option is not used.

4 Click the **Start** button.

The Throughput tool sends the specified number of data packets, in a range of packet sizes. For each data packet sent, Throughput shows the number of packets sent, the number received by the remote host, and the average time it took to receive a response (in milliseconds).

The data speed (in kilobytes per second or whatever measure is appropriate) on the connection is calculated; this is the “throughput.” This will vary depending on the system you are checking and the size of data packets.

![Throughput tool screenshot](image)

During the test, the **Start** button toggles to **Stop.** You can click **Stop** at any time to stop the test. Click **Clear** to erase the results from the display window.
Viewing Local System Information

WhatsUp provides a quick means of getting information about your local system. To view local system information, from the Tools menu, select Net Tools and click the System Info tab.

This tab displays information about your local system; WhatsUp Gold gets this information from the Windows Registry.

If your local system has multiple network adapters, System Info will display information from all of the adapters — you will see multiple IP addresses and netmasks.

Note

If you are using DHCP (Dynamic Host Configuration Protocol), the host name, IP address, domain, name server, gateway, and netmask information are dynamically assigned and the Windows registry is not updated. Therefore, the values you see in this tab (under Local Hostname, Local IP Address, Domain, Name Server, Default Gateway, and Netmask) may be incorrect or you may see zero values in place of the IP address and netmask.
Index

A
acknowledging alerts
  from console 94, 105, 110
  from web interface 147
add-ins 90
alarm colors 47, 93
alarms 94
  sounds 56, 76
  turning off 94, 105, 110
alerts
  acknowledging from
    console 94, 105, 110
  acknowledging from web
    interface 147
API for creating customized
  service checks 90
applications
  starting 32
attached lines
  disconnecting 50
  drawing 49
autorun program or script 39
B
beeper notifications 60
binary value
  searching for 87
bridges See devices.
C
captions 50
cgi program 85
checking
  definition 2
colors
  device status 4, 47, 93
  map 47
  setting 47
COM extensibility 90
COM interface 90
command line
  creating Events Reports
    with 112
  creating performance
    graphs 128
  creating Statistics Reports
    with 118
  commands on right mouse
    menu 32
  context 12, 52, 53
  custom
    devices 36
    services 90
D
db files 7
Debug Log 111
default gateway 194
dependencies 30, 98
  setting 31
  Dependencies Window 97
devices 1
  addresses 1
  alerts 74
  custom 36
  general properties of 28
  icons 40
  IPX 1
  monitoring 30
  monitoring services on 81
  names 26, 28
  status 94
  types 1
DHCP 194
disconnecting attached lines 50
Discover and Map 15, 26, 27
disk space, amount of free 194
display name 28
DNS See Domain Name
  Server.
Domain Name Server 10
domain, local 194
drawing
  shapes and lines 49
  text 50
DSN 7
E
Edit Mode 27, 48
  creating a map 25
  definition 3
e-mail notifications 62
error codes (Winsock) 95, 99
Ethernet 29
Event Log 107
  changing 105
  creating report from 109
  exporting data from 110
  types of events 104
  viewing 107
Event Report 112
Exchange service 83
  exporting data 110, 116
  exporting performance graphs
    128
  extensibility 90
F
features
  new 6
flat networks 21
free disk space 194
free memory 194
G
gateway, default 194
graphs
  performance 121
  performance, exporting
    128
  SNMP values 159
  group notifications 64
Hierarchical networks 16, 18, 20, 41, 45
host name 29
host name of local system 194
hosts See devices.
hosts file
importing devices from 16, 24
specifying 24
HTTP Content Scan 83

ICMP
network scan 21
ICMP packets 28
ICMP requests 2
icons
changing standard 40
custom device 40
names 26
IMail Server ix
importing devices 16
installation 8
upgrades 7
insufficient data 116
Internet Relay Chat 84
IP Address of local system 194
IP packet 181
Ipswitch
products ix
IPX 28, 29
IPX devices 28
polling 28
scanning 28
IRC service 84
monitoring 83

Labels 50
LANbox See devices.
lines
attached See attached
Microsoft Open Database Connectivity See ODBC.
Microsoft SQL server 83
Mini Status mode 52
Mini Status view 101
modems
drivers 70
setting up 70
Modes, Monitor and Edit 3
Monitor Mode 26
definition 3
monitoring
enabling/disabling 91
establishing the active maps 91
HTTP Content Scan 83
IRC 83
Microsoft Exchange 83
network maps 93
network type 28
polling frequency 30
Radius service 83
services 2
setting up 30
SQL service 83
using a web browser 133
using Dependencies Window 97
using map window 93
using Mini Status view 101
using Notifications Window 101
using Statistics Window 99
using Status Window 96

Name server 194
naming
icons 40
maps 51
NetBIOS 28, 29
netmask 45, 194
NetWare IPX 28
network devices See devices.
network elements See devices.
network maps See maps.
Network Neighborhood
    discovering devices from 16, 17
network type 28
networks
    flat 21
    hierarchical 18
notifications
    adding to list box 76
    assigning to devices 74
    beeper 60
    defining 56
    editing 78
    e-mail 62
    group 64
    how WhatsUp Gold stores 56
    moving to another system 56
    pager 57
    program 68
    properties 74
    receiving 94
    sharing among Ipswitch applications 56
    sound 56
    upgrading 56
    variables in 66
    viewing active 94
    voice 71
Notifications Window 101
Novell IPX See IPX.
Novell NetWare networks 28
NT service (WhatsUp Gold as) 11, 56
    starting and stopping 12
NWLink IPX/SPX Compatible Transport 28
O
    object identifiers See SNMP.
    ODBC 6, 8
P
    pager notifications 57
    parent map 18, 20, 41, 45
    performance graphs 121
        exporting 128
        samples 126
    plug-ins 90
    polling
        automatic 92
        definition 2
        dependencies 30
        frequency 30, 45
        ICMP requests 2
        methods 28
        setting dependencies 98
        starting and stopping 91
        statistics 99, 114
        stopping automatic 92
        time of day 31
        timeout 30
    port 2
    printers See devices.
    program
        notifications 68
        running automatically 39
        starting 32, 68
    properties
        devices 28
        display name 28
        host name 29
        IP address 29
        maps 44
    protocols supported 28
    Dial-In User Service 83
    reports
        event 109
        statistics 114
        using command line to create 112, 118
        requirements (system) 6
        response time See round trip time.
        right mouse menu 31, 32
        rotating
            text captions 50
        round trip time 95, 121
        routers See devices.
        RTT See round trip time.
        rules expressions
            search text 86
            text patterns 87
S
    Scan IP 26
    Scan IP tool See Scan tool.
    Scan tool 21, 45
        custom icons 40
    Scan WinNet tool 26
    scanning a network using
        SmartScan 18
        scanning the Windows network 23
    script
        running automatically 39
    search expressions 125
    services 2
        custom 90
        how they are monitored 2
        monitoring 81
        properties 81
        status 96
    Simple Network Management Protocol See SNMP.
    SmartScan 16, 18, 20, 26, 40,
    42, 45
    SNMP
concepts 150
manager 149
MIB II 149
monitoring whether SNMP is running 171
network scan 16
object identifiers 154
objects 150, 151, 154, 155, 156, 159, 160
overview 149, 150
traps 74, 94, 154, 171
sounds
quieting alarm 76, 94
recording 70
turning off alarm 76, 94
SQL server 83
starting applications 32
starting programs 32
statistics See polling statistics.
Statistics Log 114
changing 115
exporting data from 116
Statistics Reports 114
Statistics Window 99
status
device 94
message 93
network element 94
services 96
viewing 96
Status Window 96
subnet maps 18, 41, 45
loading 43
viewing 43
subnets 18, 20, 21, 41, 45
system information 194
system requirements 6
systems See devices.

T
TCP/IP 2, 6, 28
testing
installation 8
text captions
creating 50
time period 31
timeout
polling 30, 45
tips
making a map easier to read 26
toolbars
arranging 51
Traceroute tool 181
Trap Log 171
traps.txt file 154
trigger 77, 106
trigger and SNMP traps 170
U
UDP 84
Unimodem V 70
upgrading 7
keeping old notifications 56
user accounts 137
user-defined devices See devices, custom
user-defined services See services, custom.
V
variables
in notification messages 66
vendor-provided SNMP objects 154
voice modem
setting up 70
voice notifications 71
W
Web pages
customizing 135
functions 146
main page title 134
refresh frequency 134
TCP Port 134
Top View title 134
views 143
Web server
access by IP address 136, 140
customizing 135
functions 146
logging on 142
making maps available 136
setting up 133
user accounts 137
views 143
Windows registry
importing devices from 16
WinNet tool 191
Winssock errors 95, 99
Winssock information 194
WS_FTP Find Utility ix
WS_FTP Pro (FTP Client) ix
WS_FTP Scripting Utility ix
WS_FTP Server ix
WS_FTP Synchronize Utility ix
WS_Ping ProPack x
wugapi.h file 90
wugrpt.exe 112
wugrst.exe 118
wugstats.log 121
Z
zero status code 95